COMPUTER SECURITY POLICIES

HEARING

BEFORE THE

SUBCOMMITTEE ON
TRANSPORTATION, AVIATION, AND MATERIALS

OF THE

COMMITTEE ON
SCIENCE AND TECHNOLOGY
HOUSE OF REPRESENTATIVES

NINETY-NINTH CONGRESS

FIRST SESSION

JUNE 27, 1985

[No. 26]

Printed for the use of the
Committee on Science and Technology

U.S. GOVERNMENT PRINTING OFFICE
52-154 O WASHINGTON : 1985

H701-88

52-154 O - 85 - 1

COMMITTEE ON SCIENCE AND TECHNOLOGY

DON FUQUA, Florida, *Chairman*

ROBERT A. ROE, New Jersey
GEORGE E. BROWN, Jr., California
JAMES H. SCHEUER, New York
MARILYN LLOYD, Tennessee
TIMOTHY E. WIRTH, Colorado
DOUG WALGREN, Pennsylvania
DAN GLICKMAN, Kansas
ROBERT A. YOUNG, Missouri
HAROLD L. VOLKMER, Missouri
BILL NELSON, Florida
STAN LUNDINE, New York
RALPH M. HALL, Texas
DAVE McCURDY, Oklahoma
NORMAN Y. MINETA, California
MICHAEL A. ANDREWS, Texas
BUDDY MacKAY,** Florida
TIM VALENTINE, North Carolina
HARRY M. REID, Nevada
ROBERT G. TORRICELLI, New Jersey
FREDERICK C. BOUCHER, Virginia
TERRY BRUCE, Illinois
RICHARD H. STALLINGS, Idaho
BART GORDON, Tennessee
JAMES A. TRAFICANT, Jr., Ohio

MANUEL LUJAN, Jr.,* New Mexico
ROBERT S. WALKER, Pennsylvania
F. JAMES SENSENBRENNER, Jr., Wisconsin
CLAUDINE SCHNEIDER, Rhode Island
SHERWOOD L. BOEHLERT, New York
TOM LEWIS, Florida
DON RITTER, Pennsylvania
SID W. MORRISON, Washington
RON PACKARD, California
JAN MEYERS, Kansas
ROBERT C. SMITH, New Hampshire
PAUL B. HENRY, Michigan
HARRIS W. FAWELL, Illinois
WILLIAM W. COBEY, Jr., North Carolina
JOE BARTON, Texas
D. FRENCH SLAUGHTER, Jr., Virginia
DAVID S. MONSON, Utah

Harold P. Hanson, *Executive Director*
Robert C. Ketcham, *General Counsel*
Regina A. Davis, *Chief Clerk*
Joyce Gross Freiwald, *Republican Staff Director*

Subcommittee on Transportation, Aviation and Materials

GEORGE E. BROWN, Jr., California, *Chairman*

DAN GLICKMAN, Kansas
HARRY M. REID, Nevada
BILL NELSON, Florida
BART GORDON, Tennessee

TOM LEWIS, Florida
SHERWOOD L. BOEHLERT, New York
RON PACKARD, California

---

*Ranking Republican Member.
**Serving on Committee on the Budget for 99th Congress.

CONTENTS

WITNESSES

June 27, 1985: Page
- Hon. Donald C. Latham, Assistant Secretary of Defense for Command, Control, Communications and Intelligence, and Chairman, National Telecommunications and Information Systems Security Committee, U.S. Department of Defense 2
- Walter G. Deeley, Deputy Director for Communications Security and Robert L. Brotzman, Director, DOD Computer Security Center, National Security Agency, Fort Meade, MD 75
- Hon. Jack Brooks, a Representative in Congress from the State of Texas... 115
- Warren G. Reed, Director, Information Management and Technology Division, U.S. General Accounting Office, Washington, DC, accompanied by William Franklin, Associate Director; Harold Podell, Group Director, Information Management and Technology Division; and Raymond Wyrsch, senior attorney, Office of General Counsel 121
- Jerry Berman and Alan Adler, legislative counsels, American Civil Liberties Union, Washington, DC 149
- John M. Richardson, member, Committee on Communications and Information Policy, Institute of Electrical and Electronics Engineers, Inc., Washington, DC 169

COMPUTER SECURITY POLICIES

THURSDAY, JUNE 27, 1985

House of Representatives,
Committee on Science and Technology,
Subcommittee on Transportation,
Aviation and Materials,
Washington, DC.

The subcommittee met, pursuant to call, at 9:30 a.m., in room 2318, Rayburn House Office Building, Hon. Dan Glickman presiding.

Mr. Glickman. Why don't we go ahead and begin.

Mr. Lewis will be here a little later. There are a thousand things happening this morning, and so whenever he comes, his statement, he will be allowed to read it, or his statement will be in the record, whichever he chooses.

Also, Congressman Brooks is another witness that will testify today, but he will testify after Secretary Latham has completed his testimony.

And, third, we may have a rollcall vote right at 10 o'clock when we go in, in which case we would adjourn for 15 minutes. After that rollcall vote, we ought to be safe for the rest of this hearing.

And, fourth, what I usually like to do at these hearings is let witnesses feel free to summarize, because your statements will all be in the record in their entirety. However, this is a fairly technical matter, so I don't want you to feel compelled to do that. It may be more appropriate to read your testimony if you think that—particularly those from Defense and, you know, National Security Agency and others who feel more compelled to stick to the prepared text, that is fine with me as well.

I just have a small, a quick introductory statement before we begin with Secretary Latham.

Last fall the President issued a national policy on telecommunications and automated information systems security, otherwise known National Security Decision Directive 145. This directive, in my view, takes the long overdue step of creating a focus within the Government for computer and communications security, something this subcommittee has called for repeatedly.

Specifically, it creates a policy-setting structure with the broad charter of assuring the security of telecommunications and automated information systems that handle both classified and nonclassified information affecting the national security.

To carry out this objective, the directive sets up a National Telecommunications and Information Systems Security Committee, headed by an Assistant Secretary of Defense and composed of representatives from a variety of agencies. It also assigns a number of operating functions to the National Security Agency, which, if performed to their fullest, will give the NSA very great influence in this area.

Now, such a concentration of authority may be desirable. The problem is real, as our previous hearings have shown. And NSA is clearly the most technically qualified agency to attack it. But there are some who worry about allowing an arm of the military to set policy and make rules affecting other parts of the Government and the private sector, areas it may not understand very well.

Our hearing today will explore the structure and workings of this directive as it is being implemented at this time, and will examine some of the larger concerns as well.

To help us do that, we have assembled a broad cross section of expert witnesses. Their testimony will, I am sure, allow us to gain a better understanding of this new, important new thrust in Federal Government computer security.

And, as I said, just to add a couple of things, this subcommittee has held a whole series of hearings on the subject, and in fact, this afternoon I am going to be introducing some legislation dealing with the issue, although unrelated to the subject of this hearing today.

But the main thrust of this hearing that we want to talk about today is to determine whether the NSA is the appropriate agency to perform these responsibilities. And I think that involves a careful weighing of the needs of Federal agencies to have secure systems balanced with the need to know and understand the motives behind specific restrictions of data and how that affects the civilian sector.

I am, for the purposes of this committee, I am not interested, at least in these hearings, on the defense side of the picture. I am interested in the civilian side of the picture: the FAA, the Social Security Administration, veterans' records, the transfer of money in the Treasury Department, the whole issues, electric grids, power system computers. You know, a lot of these things may or may not indirectly affect national security, but most of them have a fairly clear civilian focus. And my concern is whether this directive concentrates too much power in a defense-related agency to deal with communications and computer security.

So, given that, it is a pleasure to welcome our first witness, the Hon. Donald Latham, Assistant Secretary of Defense for Command, Control, Communications and Intelligence, and the chairman of this committee, the National Telecommunications and Information Systems Security Committee.

We welcome you today, and you may begin.

STATEMENT OF HON. DONALD C. LATHAM, ASSISTANT SECRETARY OF DEFENSE FOR COMMAND, CONTROL, COMMUNICATIONS AND INTELLIGENCE, AND CHAIRMAN, NATIONAL TELECOMMUNICATIONS AND INFORMATION SYSTEMS SECURITY COMMITTEE, U.S. DEPARTMENT OF DEFENSE

Mr. **Latham**. Thank you very much, Mr. Chairman.

What I would like to do, as you suggested earlier, is have this statement for the record placed in the record. And if I may, rather than read that or anything, I have assembled a few Vu-Graphs that I thought would help structure the discussion and I would like to go through those, if I might, sir.

[Chart 1.]

What I would like to do, sir, is start out with a little background on the computer and communications security area, and give you a view of how we have structured the problem. And then I will specifically address NSDD 145 and some of the issues that you have raised; specifically, some of the policy issues.

[Chart 2.]

To do this, I would like to give you a brief look at where we see the trends going in computers and where we see the trends in telecommunications in general. It is a fact that we are seeing a blurring between those two areas such that a computer and a telecommunications network are tending to be technically one and the same, in that modern digital switches are, in fact, modern digital computers in one form or another.

I would like to tell you a little bit about the challenge that we face in this area. Then I would like to go into some of the responses, so called, that we have taken to cope with this challenge and how we are addressing that. And then I will specifically get in to the policy area and describe the NSDD 145 as it applies to to this area.

[Chart 3.]

First of all, in the computer usage trends, we are seeing an enormous increase in the usage of computers. For example, the Computer Security Agency has, in fact, evaluated and surveyed some 17,000 computers within the Department of Defense. We are now under way surveying computers across the entire Federal Government.

The term has been used "the information explosion." It is very real. We are sharing information on a global basis. We now have high-speed data links that net the world together. We have a very strong dependence on computers not only for command and control but for management and for many civilian applications, in which you have mentioned some earlier.

In addition, now we are seeing the need to introduce what we call multilevel secure networks in order to handle varying levels of security efficiently with large digital computer systems.

[Chart 4.]

In the telecommunications area, we are seeing a worldwide thrust toward open standards for information exchange. We are seeing open access to the public.

For example, there are commercial data bases available. There are technical information data bases available which some of our adversaries have, in fact, been accessing through the networks that exist on a global basis. There are, in fact, attempts to obtain Western technology through these open data bases on a real-time basis out of the computer systems.

[Chart 5.]

There is a proliferation of data networks in general, not only in the civilian world but in the Government world. We are, in fact, standardizing on a defense-data network [DOD] that has agreed-to protocols and standards. Everyone in DOD and elsewhere will use the DDN, including many civil agencies that need to share data between computers.

[Chart 6.]

You are seeing an explosion, really, in very cheap computers and cheap modems such that you can have many, many people on the air, so to speak, hooked up with phone lines and accessing systems on a global basis very easily.

[Chart 7.]

And, lastly, there is just a massive expansion of users of computer systems. There are between five and ten million personal computers now have been sold just in the United States.

[Chart 8.]

All right. The challenge, then, that we face in coping with this, the computer security—and you could say telecommunications security because I say the distinction is blurred—you must address all of these factors if you are going to talk about securing information. And the most important aspect of that is probably the third bullet, and that is the people.

[Chart 9.]

We will talk today about some of the technical aspects and what we can do, but the end result is, you must address all of these in an interlinking chain in order to really secure information.

[Chart 10.]

Specifically, if you take a typical computer network and you look at some of the vulnerabilities—I have summarized them here. These are what I would call more of the technical vulnerabilities: radiation, unintended radiation from the computer or from lines that link the computers together, hardware that is improperly connected, remote consoles in which there is access being gained illegally and people have put recorders on them, and things of that nature.

[Chart 11.]

We know how to address most of those things technically. The more important problem is, you introduce these little yellow cartoon figures here and that is where we have the greatest worry: Operators, maintenance people, tape spinners, and people like that that can gain access to these systems either through remote terminals or physically get in the computer room and, in some way, attempt to subvert the system.

So when we are talking about telecommunications and computer security, we have to address all of these factors as a systems problem.

[Chart 12.]

If you look at the risks, then, and you do a risk assessment—and this is a briefing in itself, which we can't take the time to go into today—you must address all of these factors here and some of these are very insidious.

For example, one can induce vulnerabilities into a system as it is being constructed; you may not even know it is there. In fact, it can be done so cleverly you can't even find it, and so on.

So when you are looking at the risk and assessing it, you must take into account all of these factors in looking at your response to the telecommunications and computer security area.

[Chart 13.]

One of the things we have been doing, and Mr. Deeley will discuss this in more detail, although we still consider the investments wholly inadequate, and that is the green arrow in terms of securing and doing something about our telecommunications systems, has been improving. We have a long way to go, and it is still a heavy investment area, but it is something that we have been conscious of, and are working very hard.

However, in the interactive computer network area, there hasn't been much investment, very little R&D, and as a result, as Dr. Brotzman will tell you, the risk is significant today and increasing.

[Chart 14.]

So, what are the countermeasures? What can we do in what I call an integrated response to telecommunications and computer security?

[Chart 15.]

As I mentioned, there are many links in the chain of things that you must address, and I summarize them here.

Dr. Brotzman will talk a little bit about the area of trusted computer systems, which is part of this link. Again I come back to the problem of personnel and people as probably the weakest link in the whole chain.

[Chart 16.]

So, what are we doing about it? Within the Department of Defense, anyway—and I can say now that as a result of having NSDD 145 in effect and having had several meetings with the committee, that the widespread recognition of the problem extends beyond the Department now into other agencies of the Government. I think it has been very helpful to have the NSDD promulgated.

Back in 1982, we established the Computer Security Evaluation Center, as it was titled then. Under the new NSDD, it is now the National Computer Security Center, responsible broadly for helping in this area across the entire Federal Government, as well as the civil industry.

[Chart 17.]

We have provided cryptographic devices for protection of classified data, as Mr. Deeley will explain further. While we have done a reasonable job in some areas, there are still many areas that are left uncovered and there is more emphasis needed there.

We have put in controls for tighter access to unclassified data through network access controls and things like this, so that the so-called hackers can't go in and just play havoc with our data.

[Chart 18.]

We are fostering very much a security awareness program. We are instituting training programs at the national level as well as at the local level, I'll say, within service schools and across the various agencies. And we are looking at more rigorous ways of clearing people who have access to computer systems and telecommunications network security devices.

[Chart 19.]

And then, lastly, we have established an R&D program that is centrally managed for the entire Federal Government through the security center.

We have an evaluation of vendor products under way with an approved products list available for various products. That is, if you say "I need such and such a level of protection," they will help you assess what level you need. We can then go to the products list and see what is available for providing the protection needed.

We are working with industry, as both Mr. Deeley and Dr. Brotzman will tell you, not only on cryptographic devices, secure telephones, and so on, but to inbed security into their products as they are being developed. And we are seeing very good response from industry and willingness to do that.

[Chart 20.]

Now, the recent initiatives that have been undertaken are actually in four areas. I just want to focus now on the policy area and go into what is this NSDD 145.

[Chart 21.]

The policy was promulgated back in 1984. It was quite a job getting this NSDD through the system, but I think it is a major step forward.

[Chart 22.]

What does it do? It establishes a national policy for telecommunications and automated information systems. For the first time, puts those two areas together in a policy document and sets up a Governmentwide management structure for the management of those two areas.

It establishes, as you said in your opening statement, a senior level steering group which is chaired by Mr. McFarlane, the National Security Adviser. There is the committee which I chair. The executive agent has been established as the Secretary of Defense. And for the first time, we now have a National Manager, the Director of NSA.

[Chart 23.]

The structure is as shown here, with the National Security Council in the loop directly, with Mr. McFarlane chairing the steering group, the committee then which I chair. We have had several meetings of the committee. In fact, we had an off-site retreat recently which went on for 2 days with all the agencies there to have an indepth discussion of this entire area.

[Chart 24.]

The steering group is shown here. As I mentioned, the President's Adviser for National Security Affairs is the chairman; the national manager, the Director of NSA, is executive secretary; and then the members are as shown there. Also, chaired by the Director of Science and Technology Policy, the science adviser to the President, is an NSC special coordinating subcommittee on telecommunications protection.

[Chart 25.]

The steering group is charged in the NSDD with doing these functions, and several of these are quite significant. It not only oversees the implementation of the NSDD, it monitors the activities of my committee, provides me guidance; it reports on the status of this to the President; and it recommends importantly, in that fourth bullet, recommends programs and budgets to OMB and then additional steps to improve our security in the Government.

[Chart 26.]

The committee which I chair has the membership as noted here. I would note that your concern about the military would be, I think, mitigated in the sense that the military is represented on this committee but they are in the minority.

We have a good, broad representationship across the Government. The committee has worked quite well, quite harmoniously, and we have had good responses from the other agencies.

[Chart 27.]

Now, there are two subcommittees which we have established, one on telecommunications and one on information security. Dr. Brotzman chairs one of those, the automated information systems subcommittee. These are the subcommittees, again, with representationship across all the Federal Government, that work the detailed problems.

[Chart 28.]

What am I supposed to do with this committee? It is this committee that establishes the national policy; it is not the national manager.

So I would like to dissuade you that we have empowered the director of NSA to make policy for the Federal Government in this area. It is this committee who establishes policy, the objectives and the priorities—again, being guided by the steering group.

It provides guidance to the Government departments and agencies. It gives the steering group an assessment annually of where we stand in this area. And we are about to submit to Mr. McFarlane our annual evaluation.

We identify systems which handle sensitive information. Importantly, we approve the release of sensitive system technical information and equipment, manuals and so on to foreign governments. We can have permanent and temporary subcommittees. And we have established a national issuance system of directives.

[Chart 29.]

The executive agent communication and information system security is the Secretary of Defense. He has these responsibilities as noted here. I would mention that the Secretary of Defense is not only the executive agent for communications security, but he is also for computer security, and these are the functions that he broadly performs.

I report to him directly, and keep him well aware of what is going on. In fact, yesterday the Secretary and I and the Director of NSA had lunch, and we discussed this directive as one of the luncheon topics.

[Chart 30.]

The national manager is responsible for working the details of both computer security and communications security, which is a new responsibility, as a national manager for the Director of NSA. His responsibilities are summarized here. He acts on behalf of the Secretary for the executive agent responsibilities.

[Chart 31.]

He certifies the system security. He is the focal point for all cryptographic security as he has traditionally been. He has the responsibility for liaison with foreign governments in the exchange of information in this area and equipments. He proscribes security doctrine in this area. He prepares a budget for review by the steering group. This is the first time we will do this across the Federal Government. And he prepares and executes central procurement agreements, in which today, as Mr. Deeley will point out, the procurement situation is still a decentralized appropriations of the money and a centralized procurement via funds transfers to the NSA.

[Chart 32.]

Let me summarize, then. We do believe that DOD computers containing classified information are protected by electronic means, physical means, cleared personnel and so on.

[Chart 33.]

However, numerous unclassified DOD computers exist as well as unclassified computers across the Federal Government, many of which are very vulnerable to exploitation by not just hostile intelligence services but by sixth graders, practically, with their home computers.

[Chart 34.]

A full multilevel secure system is in research and development as part of our R&D effort, and today we have some limited multilevel systems available. In the computer security jargonese, we have, I believe, one A1 system certified on the approved products list.

[Chart 35.]

The computer center is required to do these sorts of things. Dr. Brotzman will talk about these in more detail, but they are establishing standards, performing R&D, and so on, across the Federal Government.

[Chart 36.]

We are going to see that really our long-term solutions are going to have to rely heavily on industry initiatives. For example, when computer company X is designing their next generation of computer, hopefully, it will have some level like a B-1 or a B-2 built into the system as it comes off the production line and it will be on our approved products list, and can be made widely available. And the same thing is true of communications security devices.

And, last, I come back to it again, our greatest risk is still the people in the system.

Thank you very much, sir. If you have any questions, I will be glad to take those.

Mr. GLICKMAN. Thank you, Mr. Secretary.

If possible, we would like to have Xeroxes of your VuGraphs, because I think that is a good summary of your organization.

I would like, if possible, to talk for 1 minute about the organization of the committee, particularly in light of my primary concern about the problem of computer and telecommunications security and the nonclassified, civilian areas.

But as you look at your committee, you have the Secretary of Defense as the executive agent, I think you call him?

Mr. LATHAM. Yes, sir.

Mr. GLICKMAN. You have the head of NSA as the National Manager; and as I counted down the list of agencies participating, it looked like 10 of 22 agencies listed were military-related. I mean, you had the services represented——

Mr. LATHAM. The Joint Chiefs, that is five.

Mr. GLICKMAN. And I can't remember that——

Mr. LATHAM. Well, the four services, the Joint Chiefs, that is five. Then the Director of NSA sits on the committee, that is six if you want to say that is military-related. The Office of the Secretary of Defense that is on there, that is seven.

Mr. GLICKMAN. Let's see, and then there were some law enforcement—the FBI——

Mr. LATHAM. Yes; the FBI is on there, but that is a civil agency. There are actually seven, I believe, sir, of those.

Mr. GLICKMAN. OK, I could be wrong, but the fact remains that the NSA has basically taken the lead in terms of managing the committee inasmuch as the head of NSA is the—I guess you call him the National Manager

Mr. LATHAM. Well, but I am the chairman of the committee. And he just sits on the committee as another committee member, and has a vote on there like everybody else does.

Now, as a National Manager, as called out in the NSDD, he has certain prescribed functions, as I summarized on the viewgraph there, but it is not to run that committee.

Mr. GLICKMAN. OK. Do you have a charter of some sort for this committee?

Mr. LATHAM. Yes; we do.

Mr. GLICKMAN. You do have a charter?

Mr. LATHAM. Yes, sir. And we can submit that for the record.

Mr. GLICKMAN. OK, I would like to see that.

[The information follows:]

10

NTISS DIRECTIVE NO. 900
DATE: 1 MARCH 1985

NTISS
NATIONAL
TELECOMMUNICATIONS
AND
INFORMATION SYSTEMS
SECURITY

GOVERNING PROCEDURES OF THE NATIONAL TELECOMMUNICATIONS AND INFORMATION SYSTEMS SECURITY COMMITTEE

EXECUTIVE AGENT FOR NATIONAL
TELECOMMUNICATIONS AND INFORMATION SYSTEMS SECURITY

FOREWORD

National Security Decision Directive 145, dated 17 September 1984, superseded PD/NSC-24, dated 16 November 1977, while reaffirming the Secretary of Defense as the Executive Agent for Communications Security and expanding the role to include Telecommunications and Information Systems Security. It established a National Manager, the Systems Security Steering Group, and the National Telecommunications and Information Systems Security Committee (NTISSC) as an operating level interagency group.

The accompanying Directive establishes the operating procedures for the NTISSC and its two permanent subordinate subcommittees and defines the interrelationship between and among the Committee, the Systems Steering Group, the Executive Agent, and the National Manager.

This Directive supersedes National Communications Security Directive, dated 20 June 1979.

Caspar W. Weinberger
1 MAR 1985

NTISS Directive No. 900
Date:

GOVERNING PROCEDURES
# of the
NATIONAL TELECOMMUNICATIONS AND INFORMATION SYSTEMS SECURITY COMMITTEE

Section I - Establishment and Purpose

1. National Security Decision Directive (NSDD) 145, entitled "National Policy on Telecommunications and Automated Information Systems Security," dated September 17, 1984, establishes initial national objectives, policies, and an organizational structure to guide the conduct of national activities directed toward safeguarding, from hostile exploitation, systems which process or communicate sensitive information, establishes a mechanism for policy development, and assigns responsibilities for implementation. The Directive, Section 3, establishes a senior level steering group, an interagency group at the operating level, an executive agent, and a national manager to implement these objectives and policies. The National Telecommunications and Information Systems Security Committee (NTISSC) is established to operate under the direction of the Steering Group to consider technical matters and develop operating policies as necessary to implement the provisions of NSDD 145.

2. The purpose of this National Telecommunications and Informations Systems Security Directive is to establish the operating procedures governing the NTISSC and subordinate bodies as well as delineate the interrelationships between and among the Committee and the Systems Security Steering Group, the Executive Agent, and the National Manager. NSDD-145, Section 4, creates and specifies one of the responsibilities of the Systems Security Steering Group (the "Steering Group"), will be to monitor the activities of the operating level National Telecommunications and Information Systems Security Committee (the "Committee") and provide guidance for its activities.

Section II - Membership and Officers

1. The National Telecommunications and Information Systems Security Committee (NTISSC) shall be chaired by the Assistant Secretary of Defense for Command, Control, Communications and Intelligence, ASD(C3I), and be composed of voting representatives from the departments, agencies, or entities ("organizations") of those Federal Government officers designated in NSDC 145, Section 5, and listed in this Directive as Appendix A.

2. Federal Government officers, listed in Appendix A, shall designate a "representative" to serve on and attend to Committee functions, meetings, or activities. Alternate representatives will be permitted provided that advance written notification be provided to the Chairman. This written notification must identify the alternate, state that the individual will be empowered to speak for the department or agency he/she is representing and indicate the appropriate security clearance.

3. The Committee may make recommendations to the Steering Group on Committee membership. The Committee will also establish criteria and procedures for permanent observers from other departments or agencies affected by specific matters under deliberation. Qualified observers may attend Committee meetings and participate in Committee activities upon invitation of the Chair.

4. All organizations represented on the Committee, or invited to participate, shall accredit in writing to the Chair, their representatives or observers for participation in the Committee.

5. Personnel participating in the activities of the Committee, and subordinate bodies, shall possess, as a minimum, a TOP SECRET SI and TK security clearance. Written verification of security clearances shall be submitted to the Executive Secretary.

Section III - Subordinate Bodies of the NTISSC

1. The Committee shall have two permanent subordinate bodies: a Subcommittee on Telecommunications Security and a Subcommittee on Automated Information Systems Security. The subcommittees shall interact closely and any recommendations concerning implementation of protective measures shall combine and coordinate both areas as appropriate. The permanent subcommittees shall be comprised of representatives from the organizations which are represented on the Committee.

2. The Committee may establish such other permanent and temporary subordinated bodies as necessary to discharge its activities and responsibilities. These bodies may be composed of representatives or other individuals as the Committee shall select, and must be established by majority vote of the Committee.

3. Subordinate body procedures and specific responsibilities shall be governed by separate charter.

4. The Committee or the Chair, as appropriate, shall provide guidance to ensure the effective functioning of subordinate bodies.

5. The Committee shall have a permanent Executive Secretariat composed of personnel of the National Security Agency and such other personnel from organizations represented on the Committee as are requested by the Chair.

Section IV - Activities and Responsibilities

1. The activities and responsibilities of the NTISSC are directed by NSDD-145. In order to execute these activities and responsibilities the NTISSC shall:

a. develop, through attendance and participation in meetings or other activities specific operating policies, objectives, and priorities as may be required to implement NSDD-145.

b. provide telecommunication and automated information systems security guidance to the departments and agencies of the government.

c. submit annually to the Steering Group an evaluation of the status of national telecommunications and automated information systems security with respect to established objectives and priorities. Included in the evaluation will be Committee finding on the threat to and evidence of the exploitation of Government, and Government contractors telecommunications and automated information security systems.

d. identify systems which handle sensitive, non-government information, the loss and exploitation of which could adversely affect the national security interest, for the purpose of encouraging, advising and, where appropriate, assisting the private sector in applying security measures.

e. approve the release of sensitive systems technical security material, information, and techniques to foreign governments or international organizations with the concurrence of the Director of Central Intelligence for those activities which he manages.

f. establish and maintain a national system for promulgating the operating policies, directives, guidance, and disseminating advisory information which may be issued pursuant to NSDD-145. The Executive Secretary will be responsible for maintaining the NTISS issuance system in conformance with Appendix B.

g. establish permanent and temporary subcommittees as necessary to discharge the Committee responsibilities and monitor, provide guidance and direction to the subordinate bodies of the Committee.

h. make recommendations to the Steering Group on Committee membership and establish criteria and procedures for permanent observers from other departments or agencies affected by specific matters under deliberation, who may attend meetings upon invitation of the Chairman.

i. interact with the National Communications Systems Committee of Principals established by Executive Order 12472 to ensure the coordinated execution of assigned responsibilities.

2. The representatives to the Committee shall:

a. be fully empowered to act on Committee matters on behalf of their respective organizations;

b. serve as their organizations' point of contact for Committee and other matters related to the NTISSC;

c. provide complete and timely staffing of Committee actions within their organizations;

d. provide, through attendance and participation in Committee meetings, or other functions, their respective organizations' positions on matters before the Committee;

e. serve as representatives to subordinate Committee bodies at the discretion of their organizations and provide guidance to other individuals from their organizations serving on subordinate bodies;

f. provide reports, comments, or recommendations to the Committee, as required, through the Executive Secretary;

g. ensure that their respective organizations are apprised of Committee matters and other activities related to the Committee.

3. The Chair, in addition to the responsibility to keep the Executive Agent informed of significant current matters under consideration by the Committee, shall:

a. convene, preside over, and adjourn Committee meetings;

b. receive from and distribute to the Committee reports, comments, and recommendations through the Executive Secretary;

c. endorse, sign, or otherwise certify actions of the Committee; and

d. provide, through the Executive Secretary, the necessary support for Committee activities, including the timely dissemination of meeting announcements, proposed agendas, current membership rosters, and minutes of Committee meetings.

4. The Executive Secretary shall:

a. assist and provide support to the National Manager as Executive Secretary to the Systems Security Steering Group;

b. provide administrative support to the Committee and maintain official records of Committee meetings and other activities, including the assignment of serials for documents submitted to the Committee for consideration;

c. distribute correspondence to the Chair and representatives of the Committee, the Executive Agent, the National Manager, or other government organizations, as appropriate;

d. establish and maintain a national system for promulgating the operating policies, directives, guidance, or other issuances, which may be required pursuant to NSDD-145 or as the Committee or the Chair so require; and

e. maintain a current roster of the names and security clearances of all participants in the Committee and subordinate bodies, either permanent or temporary.

5. The NSA shall provide facilities and support to the Executive Secretariat as required and other organizations represented on the Committee shall provide facilities and support as requested by the Chair, through the Executive Secretary.

Section V - Meetings

1. The Chair of the Committee shall not convene a meeting unless a quorum is present. A quorum shall constitute the presence of one more than one half of the representatives.

2. The Committee shall meet at the call of the Chair or, upon request to the Chair by a majority of its representatives. The Committee should meet at least once each calendar quarter, however, a minimum of two Committee meetings shall be convened each calendar year. At the final meeting each calendar year, the Committee shall establish a tentative schedule of meetings for the forthcoming year.

3. Agenda items for Committee meetings will be submitted to the Chair through the Executive Secretary and all timely submitted agenda items shall be included on the agenda. All agenda items will be taken in the normal order of business of the meeting for which proposed, unless withdrawn by the sponsor or otherwise disposed of by vote of the representatives at the meeting. The Executive Secretary shall distribute supporting material for agenda items for review by the membership prior to meetings provided that such material is submitted to the Executive Secretary sufficiently in advance of the meeting.

4. Subordinate bodies shall meet at the call of their respective Chairs or as established by Charter as necessary to accomplish assigned tasks.

5. Except in emergency circumstances, notice of scheduled Committee meetings and proposed agendas shall be provided by the Executive Secretary ten calendar days prior to the meeting date. Additions to published agendas require approval by the meeting participants.

6. Minutes of all Committee meetings shall be prepared by the Executive Secretary and submitted to the representatives for review no later than ten working days following the meeting. The minutes shall, as a minimum, describe and record the vote on each decision made in the meeting.

7. Minutes, summaries, or reports, as appropriate, of subordinate body meetings shall be prepared by the Chair of each subordinate body. Copies shall be provided to the Executive Secretary of the Committee no later than twenty calendar days following each meeting or the final meeting, as appropriate.

Section VI - Voting

1. All representatives to the Committee shall have one vote each on matters before the Committee. The Chair shall vote in the event of a tie. All issues before the Committee will be decided, and recommendations and decisions made, by a majority vote of the representatives present and voting. Minority or dissenting views shall be recorded at the request of any representative.

2. Voting may be conducted by mail, barring written objection from any representative, in which case the Chair may call a special meeting to conduct the vote.

3. Representatives who are absent from a meeting may subsequently register, through the Executive Secretary, a formal position for the record with the Chair. Such action shall not affect the outcome of any formal vote.

4. Observers to the Committee shall neither cast votes nor be considered in determining a quorum.

5. Representatives shall neither promise nor cast proxy votes.

Section VII - Reporting Procedures

1. The Chair shall forward to the Committee and or Steering Group decisions, recommendations, findings, and recorded minority or dissenting views.

2. Representatives to the Committee shall forward, through the Executive Secretary, to the Chair copies of such implementing issuances for their respective organizations as may be required by the promulgation of NTISS policies, directives, or instructions.

3. Subordinate body reports and recommendations shall be submitted, through the Executive Secretary, to the Chair for appropriate action. The receipt of reports and recommendations by the Chair shall not signify approval. Following receipt by the Chair, the reports and recommendations shall be reviewed, formally approved or disapproved, and forwarded, as appropriate.

Appendix A

National Telecommunications and Information Systems Security Committee Membership

Chair

In accordance with Section 5 of NSDD-145, the National Telecommunications and Information Systems Security Committee shall be chaired by the Assistant Secretary of Defense for Command, Control, Communications and Intelligence.

Representatives

Membership of the Committee shall be comprised of a voting representative of each of the following:

Assistant to the President for National Security Affairs
The Secretary of State
The Secretary of the Treasury
The Secretary of Defense
Director, Office of Management and Budget
The Attorney General
The Secretary of Commerce
The Secretary of Transportation
The Secretary of Energy
Director of Central Intelligence
Chairman, Joint Chiefs of Staff
Director, National Security Agency
Administrator, General Services Administration
Director, Federal Bureau of Investigation
Director, Federal Emergency Management Agency
The Chief of Staff, United States Army
The Chief of Naval Operations
The Chief of Staff, United States Air Force
Commandant, United States Marine Corps
Director, Defense Intelligence Agency
Manager, National Communications System

APPENDIX B

NATIONAL TELECOMMUNICATIONS AND INFORMATION SYSTEMS SECURITY (NTISS) ISSUANCE SYSTEM

A National Telecommunications and Information Systems Security (NTISS) issuance system is established for purposes of promulgating objectives and policies, issuing directives and guidance, and disseminating advisory information. As a minimum, the System shall include:

1. **NTISS Policies:** May be issued by the Steering Group or the Committee through the respective Chair subsequent to approval by the members. Policy issuances reflect statements of national goals and objectives which are applicable to and binding upon the departments and agencies of the government. NTISS policies shall be issued in the following series:

001-099	General - applicable to telecommunications security (COMSEC), information systems security (COMPUSEC), and systems security countermeasures (TEMPEST).
100-199	COMSEC
200-299	COMPUSEC
300-399	TEMPEST
400-499	Reserved

2. **NTISS Directives:** These issuances are directive upon departments and agencies of the government and are promulgated by the Executive Agent, or the Chair when so delegated by the Executive Agent. Directives shall be coordinated among the representatives. Directives shall be numbered as follows:

500-599	General
600-699	COMSEC
700-799	COMPUSEC
800-899	TEMPEST
900-999	Administrative

3. **NTISS Instructions:** These issuances provide instructional guidelines and establish technical criteria on specific security matters for implementation by Committee representatives within their respective organizations. They shall be promulgated by the National Manager subsequent to coordination with the Committee and are applicable to and binding upon departments and agencies of the government. Instructions shall include technical, or implementation guidelines, restrictions, and procedures that are generally applicable to the conduct of telecommunications security and automated informations security programs or activities. They shall be numbered as follows:

1000-2999	General
3000-4999	COMSEC
5000-6999	COMPUSEC
7000-8999	TEMPEST
9000-9999	Administrative

4. **NTISS Advisory and Information Memoranda:** These issuances shall provide advice, assistance, or information of general interest to all applicable departments and agencies on matters of telecommunications security and automated information systems security and shall be issued by the National Manager. They shall be numbered as follows:

GENERAL/1-(YR) -- one-up series by year

COMSEC/1-(YR) -- one-up series by year

COMPUSEC/1-(YR) -- one-up series by year

TEMPEST/1-(YR) -- one-up series by year

NATIONAL TELECOMMUNICATIONS AND INFORMATION SYSTEMS SECURITY COMMITTEE

CHARTER

for the

SUBCOMMITTEE ON AUTOMATED INFORMATION SYSTEMS SECURITY

The National Policy on Telecommunications and Automated Information Systems Security (National Security Decision Directive 145) authorizes and directs the establishment, under the National Telecommunications and Information Systems Security Committee (NTISSC), of a permanent Subcommittee on Automated Information Systems Security (SAISS). In accordance with the policies of NSDD-145 and the Governing Procedures of the NTISSC, this Charter specifies the organization, responsibilities, and mission of the SAISS.

Matters under the cognizance of the SAISS and subject to the deliberations and actions of the SAISS include automated information systems security and other such related areas as may be determined by the subcommittee to be appropriate.

1. The Subcommittee shall be composed of one voting representative from each organization represented on the NTISSC. One alternate for each principal representative to the SAISS shall be designated to act with plenary powers in the absence of the principal. Representatives, alternates, and observers shall have a TOP SECRET/SI and TK clearance.

2. Departments, Agencies and other government organizations committed to expeditious implementation of national automated information systems security policy, and which are not represented on the NTISSC, may be invited by the Chair, NTISSC to participate in SAISS activities. Each such organization may be represented on the SAISS by an observer, who shall have all rights and privileges of representatives, except the right to vote.

3. The SAISS Chair will be the Director, National Computer Security Center. The NTISSC Secretariat also will serve as the secretariat to the SAISS.

4. The representatives to the SAISS should meet at least once per quarter each calendar year or more often at the call of the

Chair or at the request of a majority of the representatives, but not less than two times per year. A tentative agenda for each subsequent year shall be established by the Secretariat before the end of the last quarter of the current calendar year.

5. The permanent subcommittee shall have as its procedures the following:

a. The SAISS will reach decisions on matters within its cognizance by majority vote. The Chair shall vote in the event of a tie. Dissenting views, with supporting rationale, may be provided by any representative, brought to the attention of the NTISSC Secretariat, and forwarded to the full Committee.

b. Subjects for consideration by the SAISS may be referred to it by the NTISSC or by any representative to the SAISS or observer. The Secretariat will at least annually specifically solicit issues from the representatives to the SAISS for the forthcoming year.

c. The Chair will publish an agenda and summary minutes of the SAISS and its subordinate bodies which shall be the official record of business. The agenda shall be provided 10 working days before each meeting and the minutes within 10 working days after each meeting.

d. Such other procedures as may be required to conduct the chartered activities of the SAISS may be determined by the SAISS membership.

6. The SAISS is empowered to establish such temporary subordinate bodies as may be necessary to accomplish its responsibilities under the provisions of this Charter. Such bodies will establish their own procedures, but be established only for such definite term as the SAISS designates.

7. The SAISS is responsible to the full NTISSC membership for, and reports to the NTISSC Chair on:

a. Developing, formulating and recommending, for approval and establishment by the NTISSC, specific operating policies, objectives, and priorities, affecting matters under the cognizance of the SAISS as may be required to achieve the broad automated information systems security policies and objectives established by NSDD-145, or such guidance as may be subsequently issued by the Systems Security Steering Group.

b. Developing a program to work with the private sector in accordance with NSDD-145.

c. Providing a forum for the interchange of information among NTISSC member organizations, their subordinates and representatives, on all aspects of automated information systems security.

d. Evaluating annually the status of automated information systems security with respect to established objectives and policies and submit that evaluation to the Chair, NTISSC. Included in the evaluation will be information on the threat to and evidence of exploitation of U.S. Government and government contractor automated information systems.

e. Developing automated information systems security guidance for NTISSC to provide to the departments and agencies of the government. Guidance refers to direction, decision, instruction or advice which concerns automated information systems security standards, criteria, equipments, and applications.

f. Interacting with other permanent or temporary subcommittees of the NTISSC as necessary to combine, coordinate or advise on the implementation of security or protective measures where appropriate. This interaction shall take into consideration the differing levels of technology which may prevail among or between countermeasures systems.

g. Providing status reports and identifying actions and subjects which require the attention of the NTISSC in support of promoting and expediting the implementation of automated information security programs throughout the government and, insofar as it impacts on the exchange of classified or sensitive information between industry, the government, and the private sector.

h. Performing or carrying out other responsibilities relating to automated information systems security as may be directed by the NTISSC.

8. The Charter, Chairmanship and activities of the SAISS will be reviewed annually by the NTISSC.

NATIONAL TELECOMMUNICATIONS AND INFORMATION SYSTEMS SECURITY COMMITTEE

CHARTER

for the

SUBCOMMITTEE ON TELECOMMUNICATIONS SECURITY

The National Policy on Telecommunications and Automated Information Systems Security, (National Security Decision Directive 145) authorizes and directs the establishment, under the National Telecommunications and Information Systems Security Committee (NTISSC), of a permanent Subcommittee on Telecommunications Security (STS). In accordance with the policies of NSDD-145 and the Governing Procedures of the NTISSC, this Charter specifies the organization, responsibilities, and mission of the STS.

Matters under the cognizance of the STS and subject to the deliberations and actions of the STS include telecommunications technology, secure voice systems, secure record and data systems, space and satellite telecommunications systems, weapons and strategic defense telecommunications systems, command and control telecommunications systems, compromising emanations, and other such related areas as may be determined by the Subcommittee to be appropriate. The Subcommittee also subsumes the responsibilities of the former National Communications Security Committee Subcommittee on Compromising Emanations.

1. The Subcommittee shall be composed of one voting representative of each organization represented on the NTISSC. One alternate for each principal representative to STS shall be designated to act with plenary powers in the absence of the principal. Representatives, alternates, and observers shall have a TOP SECRET/SI and TK clearance.

2. Departments, Agencies and other government organizations committed to expeditious implementation of national telecommunications security policy, and which are not represented on the NTISSC, may be invited by the Chair, NTISSC to participate in STS activities. Each such organization may be represented on the STS by an observer, who shall have all rights and privileges of representatives, except the right to vote.

3. The Chair of the STS shall be the Assistant Secretary, Electronic Systems and Information Technology, Department of the Treasury. The NTISSC Secretariat also will serve as the secretariat to the STS.

4. The representatives to STS should meet at least once per quarter each calendar year or more often at the call of the Chair or at the request of a majority of the representatives, but not less than two times per year. A tentative agenda for each subsequent year shall be established by the STS Secretariat before the end of the last quarter of the current calendar year.

5. The permanent Subcommittee shall have as its procedures the following:

a. The STS will reach decisions on matters within its cognizance by majority vote. The Chair shall vote in the event of a tie. Dissenting views, with supporting rationale, may be provided by any representative, brought to the attention of the NTISSC Secretariat, and forwarded to the full Committee.

b. Subjects for consideration by the STS may be referred to it by the NTISSC or by any representative to STS or observer. The Secretariat will at least annually specifically solicit issues from the STS representative for the forthcoming year.

c. The Chair will publish an agenda and summary minutes of the STS and its subordinate bodies which shall be the official record of business. The agenda shall be provided 10 working days before each meeting and the minutes within 10 working days after each meeting.

d. Such other procedures as may be required to conduct the chartered activities of the STS may be determined by the STS membership.

6. The STS is empowered to establish such permanent or temporary subordinate bodies as may be necessary to accomplish its responsibilities under the provisions of this Charter. Such bodies will establish their own procedures, but be established only for such definite term as the STS designates.

7. The STS is responsible to the full NTISSC membership for, and reports to the NTISSC Chair on:

a. Developing, formulating and recommending, for approval and establishment by the NTISSC, specific operating policies, objectives, and priorities, affecting matters under the cognizance of the STS, as may be required to achieve the broad telecommunications security policies and objectives established by NSDD-145, or such guidance as may be subsequently issued by the Systems Security Steering Group.

b. Developing a program to work with the private sector in accordance with NSDD-145.

c. Providing a forum for the interchange of information among NTISSC members on all aspects of telecommunications security.

d. Evaluating annually the status of telecommunications systems security with respect to established objectives and policies and submit that evaluation to the Chair, NTISSC. Included in the evaluation will be information on the threat to and evidence of exploitation of U.S. Government and government contractor telecommunications systems.

e. Developing telecommunications systems security guidance for NTISSC to provide to the departments and agencies of the government. Guidance refers to direction, decision, instruction or advice which concerns telecommunications security standards, criteria, equipments, and applications.

f. Interacting with other permanent or temporary subcommittees of the NTISSC as necessary to combine, coordinate or advise on the implementation of security or protective measures where appropriate. This interaction shall take into consideration the differing levels of technology which may prevail among or between countermeasures systems.

g. Providing status reports and identifying actions and subjects which require the attention of the NTISSC in support of promoting and expediting the implementation of telecommunications security programs throughout the government and, in so far as it impacts on the operations of related communications between industry, the government, and the private sector.

h. Performing or carrying out other responsibilities relating to telecommunications security as may be directed by the NTISSC.

8. The Charter, Chairmanship and activities of the STS will be reviewed annually by the NTISSC.

Mr. GLICKMAN. So, how do you respond to the criticism that this committee is a military-oriented committee which is essentially responsible for, in many respects, civilian-related functions?

Mr. LATHAM. Well, I don't think the criticism is well-based, sir. I don't believe it is a military-dominated committee at all. I can assure you that the civil agency members on that committee are quite vocal, and are well-respected, and let their feelings be known on all matters.

Everything is done in a very structured manner before any issuance goes out, policy statement, or what have you, must be fully coordinated with each member of the committee, and worked out with them.

So, the Department of the Treasury, let's pick that one, gets an equal vote on anything that goes out of that committee, so it is, I think, well-balanced, and the civil agencies are having their say in that Committee.

Mr. GLICKMAN. OK, now the committee has been in existence for about nine months or so.

Mr. LATHAM. Well, since the NSDD was issued in September 1984, it took us a short time to get organized, but we have had several meetings since then, and it is working well, and the subcommittees have been formed, they met numerous times.

We have had a couple of issuances, and so on, since we have been——

Mr. GLICKMAN. When you say "issuances," what do you mean by that?

Mr. LATHAM. Policy documents and things of that nature. For example, at the last meeting, we agreed to a new policy statement on the security of commercial communications satellite systems, of securing certain information on those, and so on.

So, we are—it is a working body. We met for 2 days, offsite in fact, just recently, the whole committee did, and spent 2 full days working together, going over the threat, going over where we are, where we are going, and getting to know each other better.

Mr. GLICKMAN. And when you say going over the threat, you are talking about threats generically to computers and communications systems?

Mr. LATHAM. Yes, sir.

Mr. GLICKMAN. That are held by the Government.

Now, how do you explain how this directive relates to OMB's new draft circular governing computer security? We have had Mr. Wright here, Deputy Director of OMB. There may be some inconsistency.

Let me give you an example: The draft OMB circular assigns the Secretary of Commerce responsibility for issuing standards and guidance for assuring the security of Federal automated information systems.

Mr. LATHAM. Yes.

Mr. GLICKMAN. But the directive gives the responsibility to you.

Mr. LATHAM. Well, I don't think there really is any inconsistency. I would have to go see the specific language in that Draft A-71, but it is just like the National Bureau of Standards or, in this case, the Department of Commerce, they can still issue standards for telecommunications systems and what have you, and we, then, would make sure, in a review sense, working with them, that whatever standards they are issuing, are in fact the proper standards, I think would be the real interraction.

So that they are not—you know, that we don't do something dumb or at cross-purposes. They can issue the standards, but I think we now have a mechanism set up to coordinate those within the committee structure, so that whatever standard comes out, we all agree with it.

Mr. GLICKMAN. OK, now, when you say when you review them, in the organization of the committee and as a part of the directive, would the Secretary of Commerce's standards be subject to approval by the committee?

Mr. LATHAM. I would think so, in the sense that we would review them for their adequacy from a security point of view. We don't have any other authority, other than what is spelled out in the NSDD for that.

And I would think that the Commerce representative, Dr. Markey on the committee, would in fact want us to do that, so that we are all singing from the same sheet of music whenever we do promulgate a standard on information security.

Mr. GLICKMAN. OK, I would suggest that notwithstanding any of my specific questions about the relation between the military and civilian sector, that there is some confusion within the executive branch as to the role of some of these executive agencies, and how they will fit within this directive, and that that needs to be clarified through the Office of Management and Budget, because I think there probably is some confusion right now.

For example, have you at all been in contact with the Social Security Administration with respect to the security—they are making a variety of changes now in protecting information stored in their computers. Have you been involved in any of that decisionmaking there?

Mr. LATHAM. I haven't personally. Perhaps you might ask Dr. Brotzman when he is up here. Maybe the subcommittee has, in that regard.

Mr. GLICKMAN. OK.

The directive extends to unclassified but sensitive information, the loss of which could adversely affect the national security interest. I wonder how this would be defined? Because that, I think, goes to the question of the kind of information that I may be concerned about.

Mr. LATHAM. Yes, sir, that is a very good question. In fact, we are debating that very hotly within the committee structure right now, and have not come down on a completely agreed-to definition.

However, there are numerous examples of information such as that that people will agree do need protection. For example, you mentioned one, the banking information; crop information, medical record information, things of that nature we believe, while unclassified, are extremely valuable, not only to adversarial governments, but even friendly governments, perhaps, and others who may want to use that information for some purpose that could be detrimental.

So there is a class of information that we believe needs protection, and those are just three examples. And as I say, we do not have a definition I can hand you this morning that everybody in the Government signed up to yet, but we will have one.

Mr. GLICKMAN. OK, the committee will, then—will you formally adopt some sort of definition?

Mr. LATHAM. Yes, sir.

Mr. GLICKMAN. OK, I think that determining what kind of information falls into this category is going to be very necessary. At this stage, for example, would you say that information stored within computers in the Social Security Administration would be this kind of information?

Mr. LATHAM. I would, at first guess, probably say yes, because it contains a lot of personal history data that someone might find useful for some other reason. And I think people would like to have their privacy protected.

And, so, yes, I would think you would want to have some minimum level of protection to that kind of information.

Mr. GLICKMAN. To protect unclassified but sensitive data, will you need a classification system?

Mr. LATHAM. Well, we have a classification system now that delineates unclassified and so on, up to other levels. What I think we will do is we will get an agreement as to what we mean by this unclassified but sensitive information area, and one could term that a classification system, but we will have a definition of what is encompassed in that, and what isn't.

And that would, in itself, be a classification system.

Mr. GLICKMAN. Will you need levels within that?

Mr. LATHAM. I don't know whether we would or not. I would suspect we can complicate it with a bureaucratic approach like that, and that one could argue that international banking data is certainly unclassified but is also extremely sensitive, whereas the Social Security Administration data is sensitive but less sensitive.

You know, I guess somebody could come up with some levels, and in fact, what we might do is, in assessing the level of protection needed, in effect, put a classification level system in.

For example, one might want to protect banking system data with a C-2 level system, and you are willing to protect something less sensitive with a C-1 level or something like that.

Mr. GLICKMAN. OK, well, you see, I guess my concern is, is that—and I agree with you that a lot of areas fall into this nonclassified sensitive, and giving NSA and this committee kind of lead responsibility over——

Mr. LATHAM. It is the committee's responsibility to decide jointly what that is, not NSA's.

Mr. GLICKMAN. No, I realize that, but the directive came out of the—it wasn't a Department of Commerce directive, it wasn't an OMB directive, it was basically a National Security Decision Directive which did that.

So, that leads an uninformed observer like me to think that there is basically a national defense orientation to this, which may be fine, and I don't necessarily object, because I don't necessarily think there is anything wrong with it, but to do it, you need to have the specifics in your charter, the questions on what information would be covered, we need to know that there is, in fact, the kind of input from civilian agencies, which gives them, you know, a sense of equal say in a democratic type of system, and that it is an accountable system, is what I am saying.

Mr. **Latham**. Yes, I agree. It should be, absolutely should be.

Mr. **Glickman**. OK.

How would you characterize the relative size and difficulty of the jobs facing you in computer and in communications security?

Mr. **Latham**. Let me take those in two parts.

The telecommunications security area is a matter of a much more aggressive investment program, more so than inventing some new technology or some new, radical approaches.

As Mr. Deeley will point out to you in some detail, the issue has been a lack of a national will, so to speak, to secure up our information systems and our telecommunications systems over a long period of time, and as a result, we are being bled to death by people who are taking out technology information and other things.

So, it is a matter of investment, because the devices and the technology are here to do that, and that is dollars, and people being willing to do it.

The other area, the computer security area, is an area which requires an enormous R&D program to understand and build the kind of systems and procedures that we can really safely safeguard information against hostile attacks.

So, it is in its infancy, as Dr. Brotzman will tell you, we need a number of things invented. We don't know how to build, for example, what is called an A-2 level system yet. We are working on that, where you could have an unclassified person at a terminal accessing a computer system that hosted a much higher classification information.

So, there is a fair amount of invention needed in the computer security area, not so much in the telecommunications area. We are facing a dollar investment issue, and a significant R&D effort in that area, too.

Mr. **Glickman**. OK, tough problem.

Let me just ask you two final questions. One questions relates to how this directive got started in the first place. In the Government scheme of things, who are the responsible parties that made the decision to move ahead in this direction?

Mr. **Latham**. OK, in the Carter administration, as you may recall, there was a directive called a PD-24, which was a Presidential directive dealing just with communications security. It did not have wrapped into it the computer security area, nor did it set up a management structure or anything like that.

When I came on board in 1981, one of the first things I started, from my office, was the rewrite of PD-24, and so we took the initiative to push the rewrite of that, and frankly, it took us a couple of years of working it with the National Security Council, or working it with the various Federal agencies, the OMB, yes, NSA, to finally arrive at this NSDD 145, which we pushed very hard for to encompass both the telecommunications and the computer security, and set up the management structure.

It was a very difficult job pushing this through the Government.

Mr. **Glickman**. But was there a vote in the National Security Council?

Mr. **Latham**. No, I don't believe there was any vote at a Council meeting, or anything like that. They played a very strong role in helping us formulate the NSDD, and seeking the approval within the NSC for this document.

Mr. **Glickman**. What about the President's Cabinet? Do you know if there was ever discussion of this in a Cabinet meeting?

Mr. **Latham**. I don't believe there was, sir.

Mr. **Glickman**. What I am just trying to figure out is that you have established a kind of cross-jurisdictional group to provide protection for communications and computer security that is basically chaired by yourself and the executive managers, the head of the NSA, it has civilian agency input.

And I wonder whether in the process of developing the format for this organization, whether there was a kind of joint sharing of decisionmaking, or whether it was pretty much internal within your shop?

Mr. **Latham**. Oh, I can tell you that we had some meetings over in the old Executive Office Building at which all the civilian agencies participated. It was chaired by the Deputy National Security Council individual, and it was hotly discussed. This thing was very well-discussed at all the senior levels.

It did not go to a Cabinet meeting, but certainly Cabinet-level officers were aware of it going on. Mr. Weinberger certainly was, and I am sure that other senior Cabinet members were aware, because of their members telling them what was going on, because it had significant implications, as you are implying, for restructuring and managing this area.

But we did finally get unanimous agreement to go ahead with it as it is.

Mr. **Glickman**. OK, in your charter, I hope that you will, if you don't now, have some focus for privacy considerations. That is, you know, DOD is obviously concerned, as it should be, and NSA, with security concerns affecting the national security of the United States.

Mr. **Latham**. It doesn't explicitly go into details on privacy. I am not sure where we should put that. We possibly could include it as an additional area, but I would say that that has been discussed in the committee, and everybody is keenly aware of the issue of privacy and protection of the individual's rights, and so on.

And one of the things that we have tried to do is not only to involve the Federal agencies in some of these decisions, but involve the industry, in general, and the public, in general. Specifically, in the discussion of the security of telecommunications satellites, commercial communications satellites, and perhaps other satellite systems, nonmilitary, we went out and solicited views of the public in general, and of the industry specifically as to how they viewed that particular policy document.

And we intend to do that in all of these areas, so that we make sure that we are, in fact, reflecting the will of the people, you could say, and not just a narrow view taken by some bureaucratic committee.

Mr. **Glickman**. Well, I hope that you will consider, as you review your charter, and the organization, some specific reference to privacy statutes——

Mr. **Latham**. All right, I will take that as an action item.

Mr. **Glickman**. Because, you see, even with respect to changing technologies, functions that we just automatically assumed were protected with respect to individuals may not be, as we move into all forms of exotic technologies, and I just think it is important that if you are going to be doing this thing, that you at least appear that you have this as one of your basic focuses.

Mr. **Latham**. Well, let me give you an example: Suppose you find that some—and there was one—entry into one particular hospital's medical records. You would like, I think, to protect your own personal medical records, because the insidious situation is someone can get in and alter your record.

So that form of protection of your privacy is very important, and yet you are going to have to be a little bit relaxed at this protection system that someone would impose, let's say, on a medical records system. In fact in your best interest, and in the public's best interest, which I think it is.

Mr. **Glickman**. That's right. Well, what I would like to tell people, is you, Secretary Latham, should assume that not only are you protecting the Government and the Government's records and Government security, but your own personal record.

Mr. **Latham**. Yes, sir.

Mr. **Glickman**. Part of the same process as well.

Mr. **Latham**. Yes, sir.

Mr. **Glickman**. OK. We appreciate your testimony. Thank you very much.

Mr. **Latham**. Thank you.

[The charts mentioned in testimony, plus the prepared statement of Mr. Latham follows:]

ID1544, PENTAGON, D87504.59 • 17 OCT 83

COMPUTER
AND
TELECOMMUNICATIONS
SECURITY

Challenges and Responses

ID1329, PENTAGON, D87504.13 • 17 OCT 83

DISCUSSION OUTLINE

- BACKGROUND
  - COMPUTER AND TELECOMMUNICATIONS TRENDS
- THE CHALLENGE
  - VULNERABILITIES
  - THREAT
  - RISK
- TRUSTED SYSTEMS: THE RESPONSE
  - INFORMATION PROTECTION
  - COMPUTER SECURITY EVALUATION CENTER
  - INITIATIVES
- OBSERVATIONS

ID1329, PENTAGON, D87504.21 • 17 OCT 83

COMPUTER USAGE TRENDS

- INCREDIBLE GROWTH IN QUANTITY OF DATA AVAILABLE
  - LOW COST MASS STORAGE
- INFORMATION SHARING
  - GLOBAL BASIS - RAPID ACCESS
- COMPARTMENTATION OF DATA
- DEPENDENCE
  - FOR C^2 - FOR WEAPONS - MANAGEMENT
- INTRODUCTION OF MULTI SECURITY LEVEL SYSTEMS
  - PRODUCTIVITY - NETWORKING (e.g., SACDIN)

ID1329, PENTAGON, D87504.18 • 17 OCT 83

TELECOMMUNICATIONS TRENDS FOR UNCLASSIFIED SYSTEMS AND NETWORKS

- WORLDWIDE THRUST TOWARD STANDARDS FOR INFORMATION INTERCHANGE IN AN OPEN SYSTEMS ENVIRONMENT (ISO REFERENCE MODEL)
- OPEN ACCESS TO THE PUBLIC
  - COMMERCIAL DATA BASES (Example: NEXIS)
  - TECHNICAL INFORMATION DATA BASES
    - GOVERNMENT (NTIC)
    - COMMERCIAL (DIALOG)

ID1329, PENTAGON, D87504.17 • 17 OCT 83

TELECOMMUNICATIONS TRENDS FOR UNCLASSIFIED SYSTEMS AND NETWORKS

- WORLDWIDE THRUST TOWARD STANDARDS FOR INFORMATION INTERCHANGE IN AN OPEN SYSTEMS ENVIRONMENT (ISO REFERENCE MODEL)
- OPEN ACCESS TO THE PUBLIC
  - COMMERCIAL DATA BASES (Example: NEXIS)
  - TECHNICAL INFORMATION DATA BASES
    - GOVERNMENT (NTIC)
    - COMMERCIAL (DIALOG)
- SIGNIFICANT PROLIFERATION OF DATA NETWORKS IN GENERAL
  - COMMERCIAL
  - DOD

ID1329, PENTAGON, D87504.16 • 17 OCT 83

TELECOMMUNICATIONS TRENDS FOR UNCLASSIFIED SYSTEMS AND NETWORKS

- WORLDWIDE THRUST TOWARD STANDARDS FOR INFORMATION INTERCHANGE IN AN OPEN SYSTEMS ENVIRONMENT (ISO REFERENCE MODEL)
- OPEN ACCESS TO THE PUBLIC
  - COMMERCIAL DATA BASES (Example: NEXIS)
  - TECHNICAL INFORMATION DATA BASES
    - GOVERNMENT (NTIC)
    - COMMERCIAL (DIALOG)
- SIGNIFICANT PROLIFERATION OF DATA NETWORKS IN GENERAL
  - COMMERCIAL
  - DOD
- CHEAP COMPUTER TERMINALS AND COMM MODEMS

ID1329, PENTAGON, D87504.15 • 17 OCT 83

TELECOMMUNICATIONS TRENDS FOR UNCLASSIFIED SYSTEMS AND NETWORKS

- WORLDWIDE THRUST TOWARD STANDARDS FOR INFORMATION INTERCHANGE IN AN OPEN SYSTEMS ENVIRONMENT (ISO REFERENCE MODEL)
- OPEN ACCESS TO THE PUBLIC
  - COMMERCIAL DATA BASES (Example: NEXIS)
  - TECHNICAL INFORMATION DATA BASES
    - GOVERNMENT (NTIC)
    - COMMERCIAL (DIALOG)
- SIGNIFICANT PROLIFERATION OF DATA NETWORKS IN GENERAL
  - COMMERCIAL
  - DOD
- CHEAP COMPUTER TERMINALS AND COMM MODEMS
- **MASSIVE EXPANSION OF USERS**

ID1544, PENTAGON, D87504.58 • 17 OCT 83

THE CHALLENGE

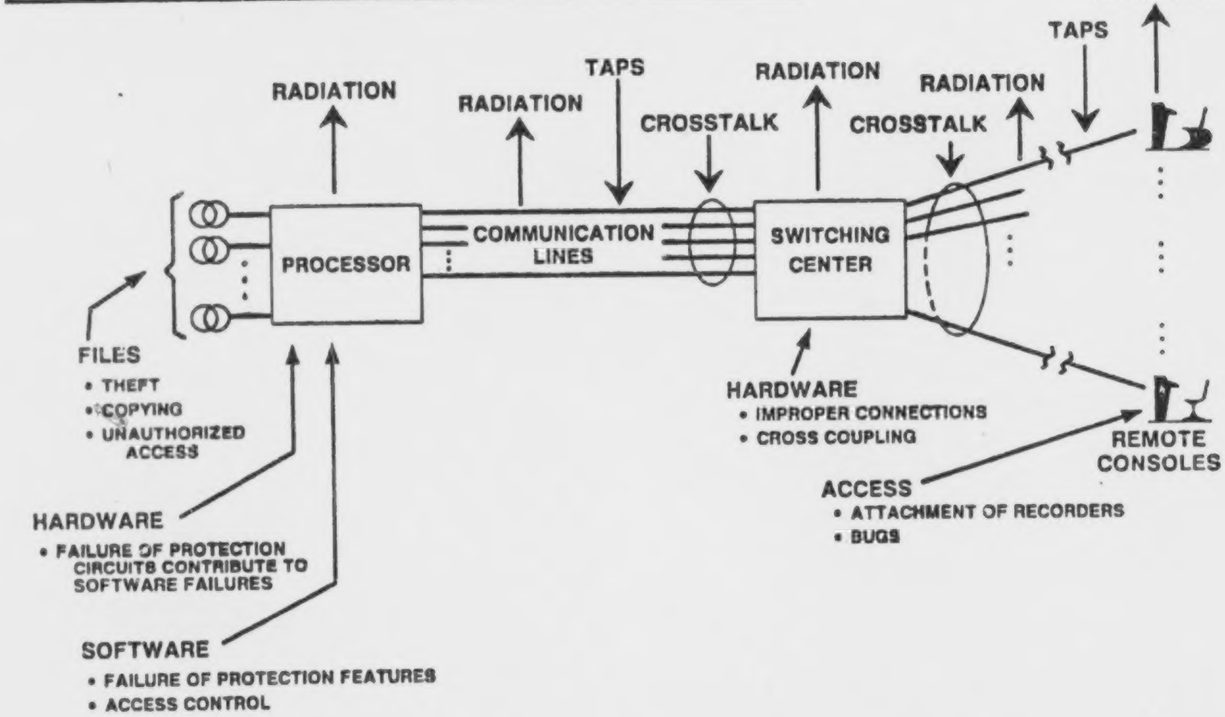
ID1329, PENTAGON, D87504.19 • 17 OCT 83

COMPUTER SECURITY
A MULTIFACETED SECURITY CHALLENGE

- PHYSICAL
- ADMINISTRATIVE
- PERSONNEL
- COMMUNICATIONS
- EMANATIONS
- HARDWARE / SOFTWARE

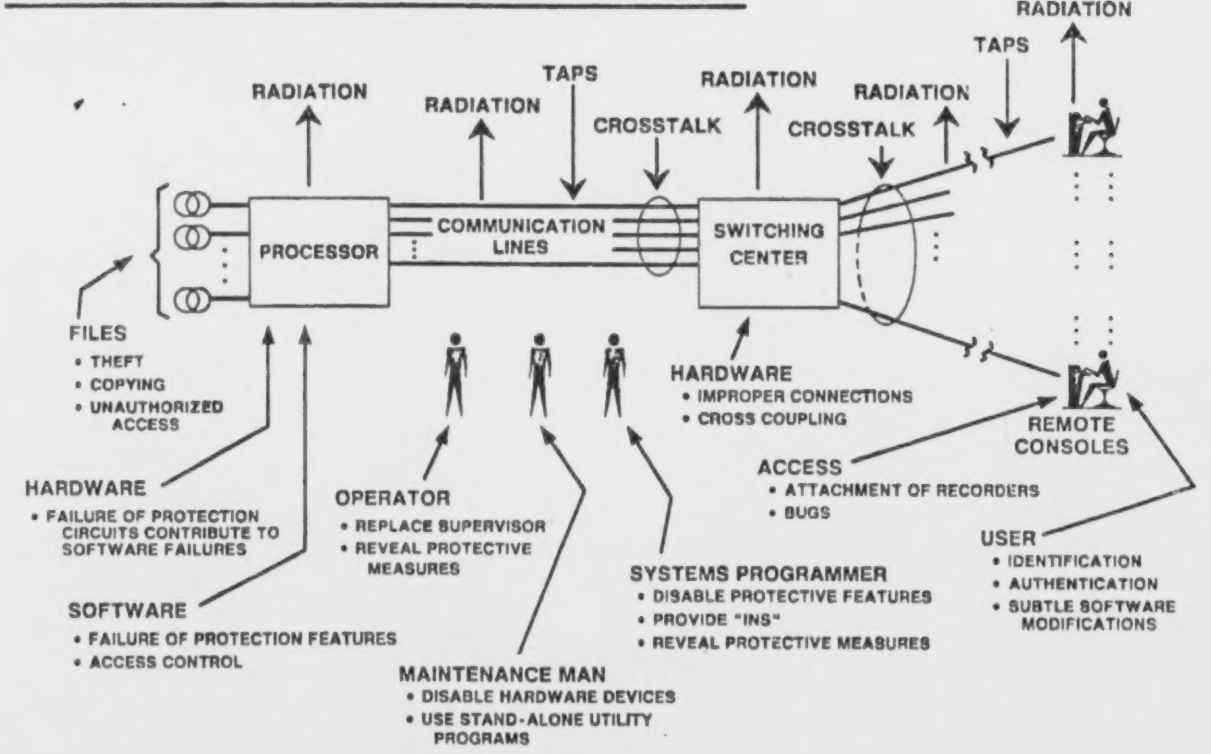
ID1544, PENTAGON, D87504.85 • • 17 OCT 83

COMPUTER NETWORK VULNERABILITIES


RADIATION
RADIATION
TAPS
CROSSTALK
RADIATION
RADIATION
CROSSTALK
TAPS
RADIATION
PROCESSOR
COMMUNICATION LINES
SWITCHING CENTER
FILES
• THEFT
• COPYING
• UNAUTHORIZED ACCESS
HARDWARE
• FAILURE OF PROTECTION CIRCUITS CONTRIBUTE TO SOFTWARE FAILURES
SOFTWARE
• FAILURE OF PROTECTION FEATURES
• ACCESS CONTROL
HARDWARE
• IMPROPER CONNECTIONS
• CROSS COUPLING
ACCESS
• ATTACHMENT OF RECORDERS
• BUGS
REMOTE CONSOLES

ID1544, PENTAGON, D87504.84 • • 17 OCT 83

COMPUTER NETWORK VULNERABILITIES



RADIATION
RADIATION
TAPS
RADIATION
CROSSTALK
CROSSTALK
RADIATION
TAPS
RADIATION
PROCESSOR
COMMUNICATION LINES
SWITCHING CENTER
REMOTE CONSOLES

FILES
- THEFT
- COPYING
- UNAUTHORIZED ACCESS

HARDWARE
- FAILURE OF PROTECTION CIRCUITS CONTRIBUTE TO SOFTWARE FAILURES

SOFTWARE
- FAILURE OF PROTECTION FEATURES
- ACCESS CONTROL

OPERATOR
- REPLACE SUPERVISOR
- REVEAL PROTECTIVE MEASURES

MAINTENANCE MAN
- DISABLE HARDWARE DEVICES
- USE STAND-ALONE UTILITY PROGRAMS

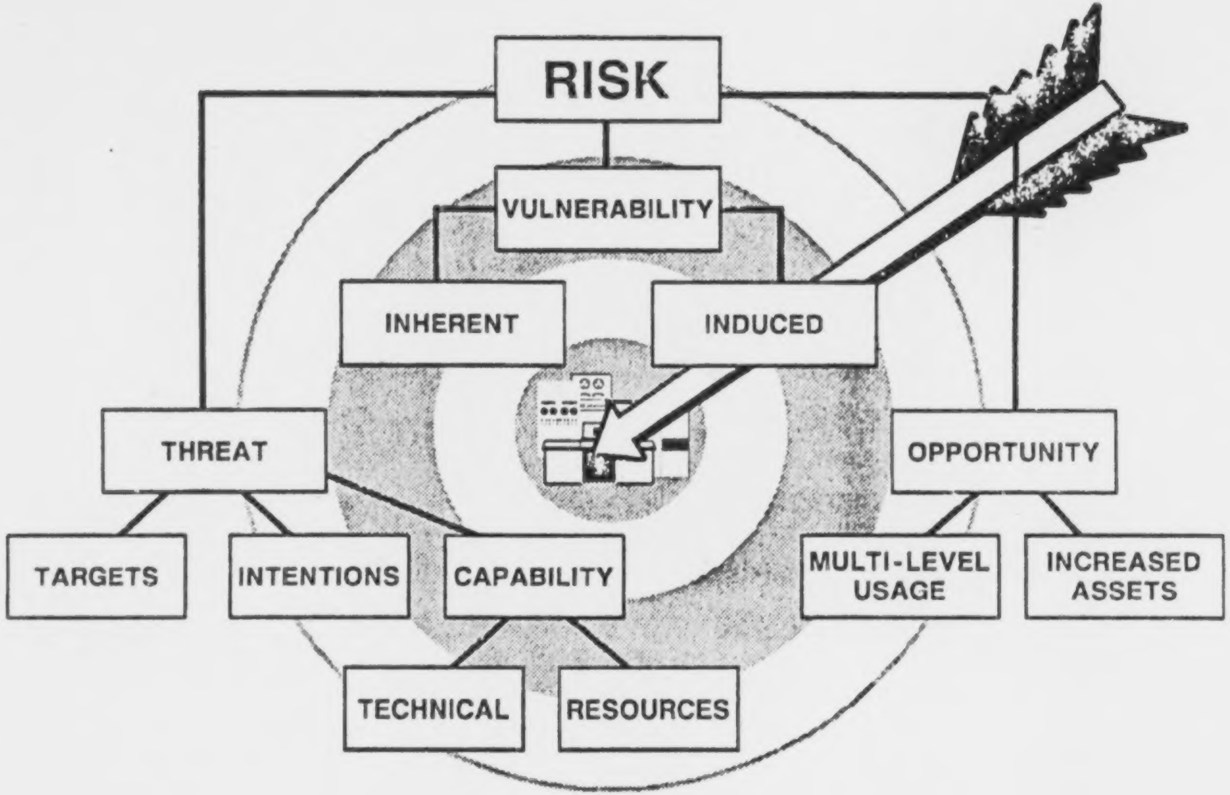
SYSTEMS PROGRAMMER
- DISABLE PROTECTIVE FEATURES
- PROVIDE "INS"
- REVEAL PROTECTIVE MEASURES

HARDWARE
- IMPROPER CONNECTIONS
- CROSS COUPLING

ACCESS
- ATTACHMENT OF RECORDERS
- BUGS

USER
- IDENTIFICATION
- AUTHENTICATION
- SUBTLE SOFTWARE MODIFICATIONS

ID1544, PENTAGON, D87504.83 • • 17 OCT 83



RISK

VULNERABILITY

INHERENT

INDUCED

THREAT

TARGETS

INTENTIONS

CAPABILITY

TECHNICAL

RESOURCES

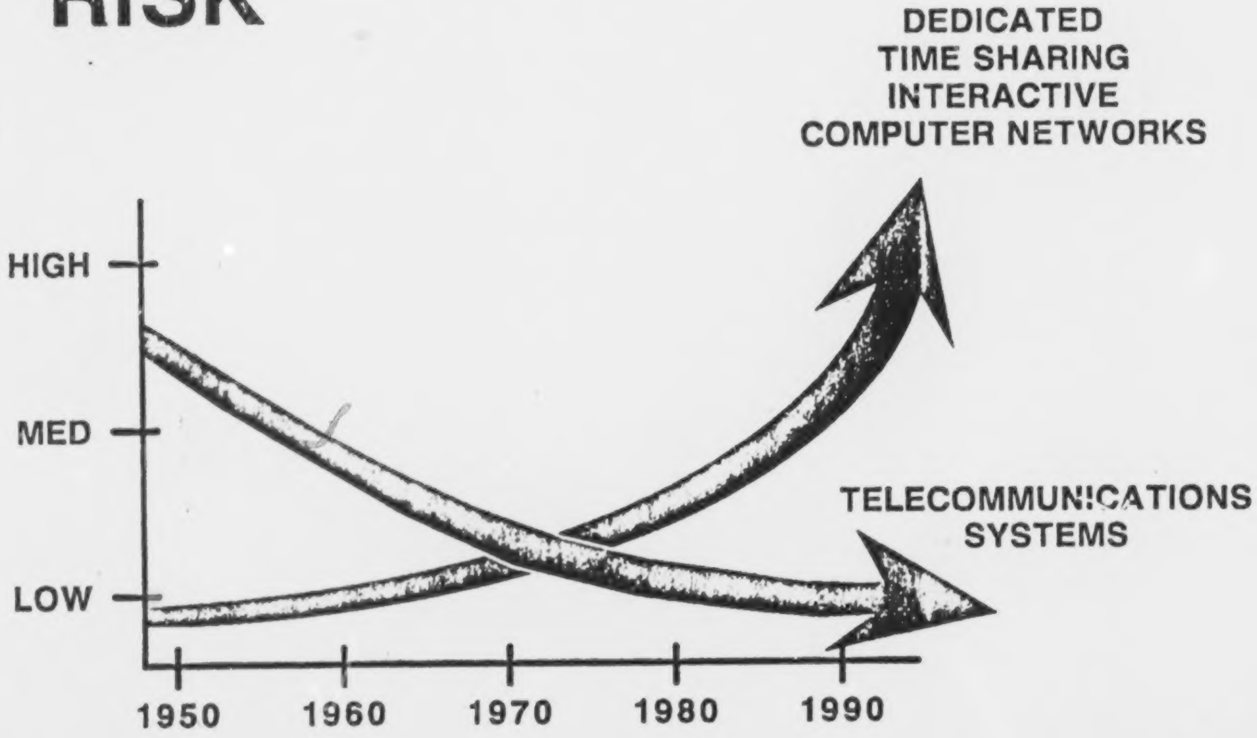
OPPORTUNITY

MULTI-LEVEL USAGE

INCREASED ASSETS

iD1544, PENTAGON, D87504.82 • 17 OCT 83

RISK

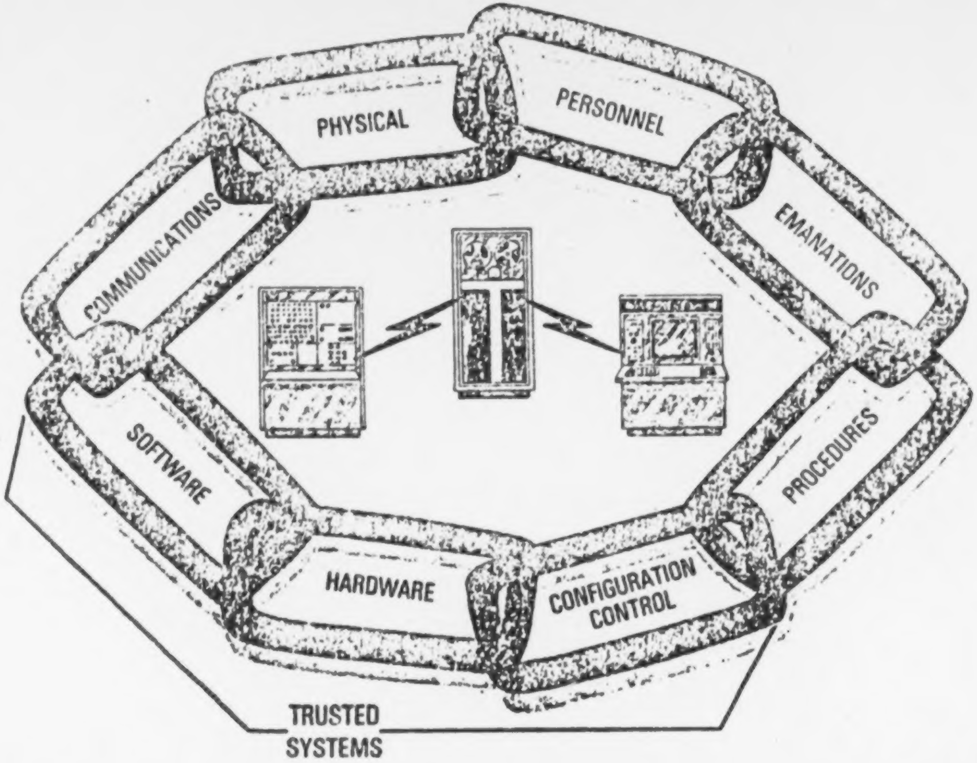


ID1544, PENTAGON, D87504.60 17 OCT 83

“COUNTERMEASURES“

An Integrated Response to
Computer Security and
Telecommunications Security

INFORMATION PROTECTION


PHYSICAL
PERSONNEL
EMANATIONS
PROCEDURES
CONFIGURATION CONTROL
HARDWARE
SOFTWARE
COMMUNICATIONS
TRUSTED SYSTEMS

WHAT ARE WE DOING ABOUT THIS PROBLEM

- WIDESPREAD PROBLEM RECOGNITION IN DOD
- ESTABLISHMENT OF DOD COMPUTER SECURITY EVALUATION CENTER IN 1982

ID1329, PENTAGON, D87504.25 • 17 OCT 83

WHAT ARE WE DOING ABOUT THIS PROBLEM

- WIDESPREAD PROBLEM RECOGNITION IN DOD
- ESTABLISHMENT OF DOD COMPUTER SECURITY EVALUATION CENTER IN 1982
- CRYPTOGRAPHIC PROTECTION OF CLASSIFIED DATA
- TIGHTER ACCESS TO UNCLASSIFIED DATA THROUGH NETWORK ACCESS CONTROLS

WHAT ARE WE DOING ABOUT THIS PROBLEM

- WIDESPREAD PROBLEM RECOGNITION IN DOD
- ESTABLISHMENT OF DOD COMPUTER SECURITY EVALUATION CENTER IN 1982
- CRYPTOGRAPHIC PROTECTION OF CLASSIFIED DATA
- TIGHTER ACCESS TO UNCLASSIFIED DATA THROUGH NETWORK ACCESS CONTROLS
- FOSTERING COMPUTER SECURITY AWARENESS THROUGH TRAINING PROGRAMS
- CONTINUING RIGOROUS PERSONNEL CLEARANCE PROCEDURES

ID1329, PENTAGON, D87504.23 • 17 OCT 83

WHAT ARE WE DOING ABOUT THIS PROBLEM

- WIDESPREAD PROBLEM RECOGNITION IN DOD
- ESTABLISHMENT OF DOD COMPUTER SECURITY EVALUATION CENTER IN 1982
- CRYPTOGRAPHIC PROTECTION OF CLASSIFIED DATA
- TIGHTER ACCESS TO UNCLASSIFIED DATA THROUGH NETWORK ACCESS CONTROLS
- FOSTERING COMPUTER SECURITY AWARENESS THROUGH TRAINING PROGRAMS
- CONTINUING RIGOROUS PERSONNEL CLEARANCE PROCEDURES
- **TECHNICAL R&D COMPUTER SECURITY PROGRAM, CENTRALLY MANAGED**
- **EVALUATION OF VENDOR PRODUCTS**
- **WORKING WITH INDUSTRY TO GAIN MORE SECURE COMMERCIAL PRODUCTS**

ID1554, PENTAGON, D87504.93 • 19 APR 84

RECENT INITIATIVES

POLICY

ADMINISTRATIVE

TECHNICAL

AWARENESS

ID156.S,MACMILLIAN-S07,T4101.2 04SEP84

NATIONAL SECURITY DECISION DIRECTIVE (NSDD)
NO. 145

NATIONAL POLICY ON TELECOMMUNICATIONS AND AUTOMATED INFORMATION SYSTEMS SECURITY

17 SEPTEMBER 1984

ID 2027, PENTAGON, D65860.1

18 OCT 84

POLICY

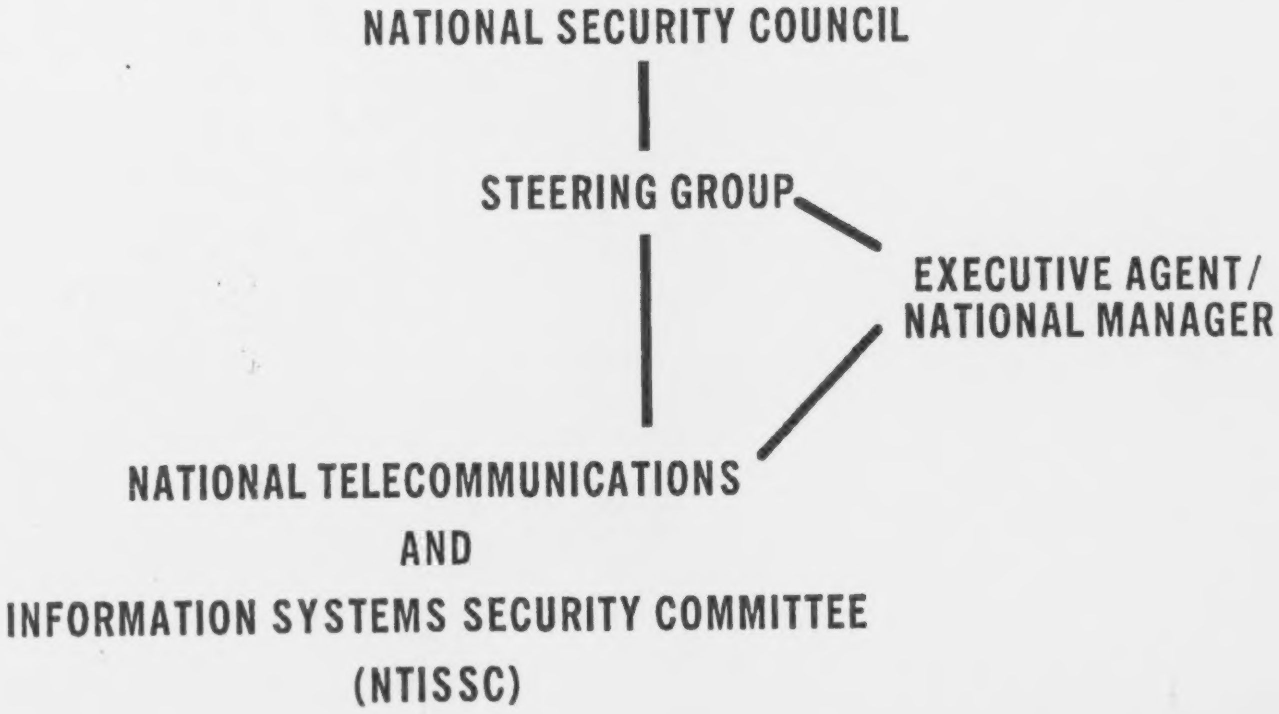
NATIONAL POLICY ON TELECOMMUNICATIONS AND AUTOMATED INFORMATION SYSTEMS (AIS) SECURITY (NSDD-145)

- MAINTAIN OR IMPROVE AIS'S AGAINST TECHNICAL EXPLOITATION THREATS
- MANAGEMENT STRUCTURE
  - SENIOR LEVEL STEERING GROUP - CHAIR (ASSISTANT TO PRESIDENT FOR NATIONAL SECURITY AFFAIRS)
  - NATIONAL TELECOMMUNICATIONS AND INFORMATION SYSTEM SECURITY COMMITTEE - CHAIR (ASD(C3I))
  - EXECUTIVE AGENT - SECDEF
  - NATIONAL MANAGER - NSA

2027-D65860.1

ID156.S,MACMILLIAN(DALEY)-S08,T4200.2

20SEP84



NATIONAL SECURITY COUNCIL

STEERING GROUP

EXECUTIVE AGENT/
NATIONAL MANAGER

NATIONAL TELECOMMUNICATIONS
AND
INFORMATION SYSTEMS SECURITY COMMITTEE
(NTISSC)

ID156.S,MACMILLIAN(DALEY)-S08,T4200.3 20SEP84

NSC SYSTEMS SECURITY STEERING GROUP

CHAIRMAN: PRESIDENT'S ADVISOR FOR NATIONAL SECURITY AFFAIRS

EXEC SEC: NATIONAL MANAGER

MEMBERS:
- STATE
- TREASURY
- SECRETARY OF DEFENSE (EXEC AGENT)
- DCI
- OMB
- ATTORNEY GENERAL

NSC SPECIAL COORDINATION COMMITTEE SUBCOMMITTEE ON TELECOMMUNICATIONS PROTECTION

CHAIRMAN: DIRECTOR, OFFICE OF SCIENCE AND TECHNOLOGY POLICY

MEMBERS:
- STATE
- TREASURY
- JUSTICE
- COMMERCE
- DEFENSE
- TRANSPORTATION
- ENERGY
- CIA
- GSA
- NSA
- NSC STAFF

ID156.S,MACMILLIAN(DALEY)-S08,T4200.4 20SEP84

SYSTEMS SECURITY STEERING GROUP

- OVERSEE NSDD IMPLEMENTATION
- MONITOR ACTIVITIES AND PROVIDE GUIDANCE TO NTISSC
- REPORT STATUS OF INFORMATION SYSTEMS SECURITY TO THE PRESIDENT
- SUBMIT RECOMMENDED PROGRAMS AND BUDGETS TO OMB
- IDENTIFY AND RECOMMEND STEPS TO PROTECT NON-GOVERNMENT, SENSITIVE INFORMATION

ID156.S,MACMILLIAN-S07,T4101.5

04SEP84

NATIONAL TELECOMMUNICATIONS AND INFORMATION SYSTEMS SECURITY COMMITTEE (NTISSC)

CHAIRMAN: ASSISTANT SECRETARY OF DEFENSE C3I
SECRETARIAT: NSA

MEMBERS:

- NSC
- STATE
- TREASURY
- DoD
- DCI
- OMB
- ATTORNEY GENERAL
- COMMERCE
- TRANSPORTATION
- ENERGY
- GSA
- JCS
- ARMY
- NAVY
- AIR FORCE
- MARINE CORPS
- NSA
- DIA
- FBI
- FEMA
- NCS

ID156.S,MACMILLIAN-S07,T4101.7

04SEP84

NTISSC - SUBCOMMITTEES

TELECOMMUNICATIONS SECURITY

AUTOMATED INFORMATION SYSTEMS SECURITY

NATIONAL TELECOMMUNICATIONS AND INFORMATION SYSTEMS SECURITY COMMITTEE

- ESTABLISH NATIONAL POLICY, OBJECTIVES, AND PRIORITIES
- PROVIDE GUIDANCE TO GOVERNMENT DEPARTMENTS AND AGENCIES
- PROVIDE THE STEERING GROUP WITH AN ANNUAL EVALUATION ON THE STATUS OF INFORMATION SYSTEMS SECURITY
- IDENTIFY SYSTEMS WHICH HANDLE SENSITIVE NON-GOVERNMENT INFORMATION WHICH NEED PROTECTING AND RECOMMEND SOLUTIONS
- APPROVE FOREIGN RELEASE OF SENSITIVE SYSTEM TECHNICAL SECURITY MATERIAL, INFORMATION, AND TECHNIQUES
- ESTABLISH PERMANENT AND TEMPORARY SUBCOMMITTEES
- ESTABLISH AND MAINTAIN A NATIONAL ISSUANCE SYSTEM

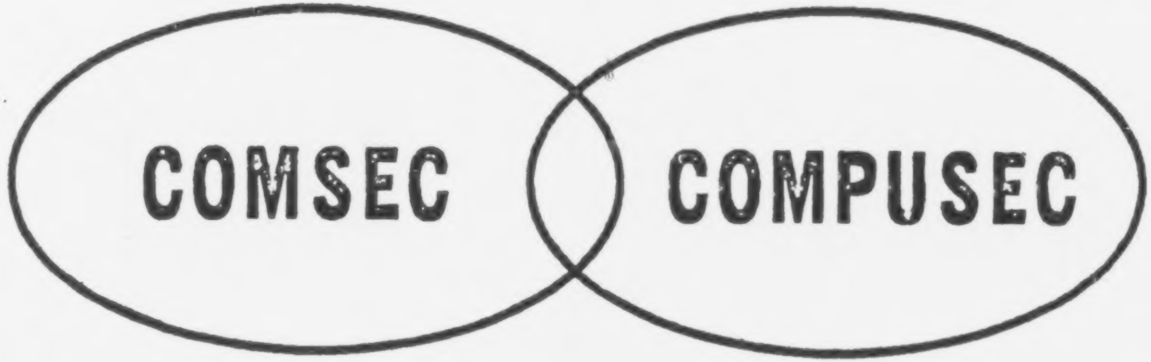
EXECUTIVE AGENT: SECRETARY OF DEFENSE

- DEVELOP PLANS & PROGRAMS IN CONJUNCTION WITH NTISSC
- OVERSEE CENTRAL PROCUREMENT FOR GOVERNMENT AND, WHEN APPROPRIATE, CIVIL SECTOR
- ISSUE SECURITY DOCTRINE AND STANDARDS
- ENSURE THE CONDUCT OR APPROVE OR ENDORSE TELECOMMUNICATIONS & AUTOMATED INFORMATION SYSTEMS R & D
- MANAGE TELECOMMUNICATIONS & AUTOMATED INFORMATION SECURITY ACTIVITIES
- DEVELOP PROGRAMS AND BUDGETS FOR SUBMISSION TO THE STEERING GROUP

ID156.S,MACMILLIAN-S08,C4419.2

26OCT84

NATIONAL MANAGER



COMSEC

COMPUSEC

NSA

NATIONAL MANAGER: DIRECTOR, NSA

- ACTS ON BEHALF OF SEC DEF IN CARRYING OUT EXECUTIVE AGENT RESPONSIBILITIES
- VULNERABILITY & SECURITY SYSTEMS EVALUATION
- FOCAL POINT FOR CRYPTOGRAPHIC SECURITY
- CERTIFY SECURITY SYSTEMS
- LIAISON, INCLUDING AGREEMENTS, WITH FOREIGN GOVERNMENTS, INTERNATIONAL, AND PRIVATE ORGANIZATIONS
- PRESCRIBE SECURITY DOCTRINE AND STANDARDS
- PREPARE TELECOMMUNICATIONS SECURITY BUDGET & REVIEW AUTOMATED INFORMATION SECURITY BUDGET
- PREPARE AND EXECUTE PROCUREMENT AGREEEMENTS
- OPERATE PRINTING AND FABRICATION FACILITIES

ID1329, PENTAGON, D87504.7 • 17 OCT 83

OBSERVATIONS

- DOD COMPUTERS CONTAINING CLASSIFIED DATA ARE PROTECTED
  - ELECTRONICALLY
  - PHYSICALLY
  - CLEARED PERSONNEL

ID1329, PENTAGON, D87504.6 • 17 OCT 83

OBSERVATIONS

- DOD COMPUTERS CONTAINING CLASSIFIED DATA ARE PROTECTED
  - ELECTRONICALLY
  - PHYSICALLY
  - CLEARED PERSONNEL
- THE NUMEROUS UNCLASSIFIED DOD COMPUTER SYSTEMS ARE MUCH MORE VULNERABLE TO HOSTILE EXPLOITATION

OBSERVATIONS

- DOD COMPUTERS CONTAINING CLASSIFIED DATA ARE PROTECTED
  - ELECTRONICALLY - PHYSICALLY - CLEARED PERSONNEL
- THE NUMEROUS UNCLASSIFIED DOD COMPUTER SYSTEMS ARE MUCH MORE VULNERABLE TO HOSTILE EXPLOITATION
- FULL MULTILEVEL SECURE SYSTEMS ARE IN R&D
  - LIMITED MULTILEVEL SYSTEMS ARE AVAILABLE

ID1329, PENTAGON, D87504.4 • 17 OCT 83

OBSERVATIONS

- DOD COMPUTERS CONTAINING CLASSIFIED DATA ARE PROTECTED
  - ELECTRONICALLY
  - PHYSICALLY
  - CLEARED PERSONNEL
- THE NUMEROUS UNCLASSIFIED DOD COMPUTER SYSTEMS ARE MUCH MORE VULNERABLE TO HOSTILE EXPLOITATION
- FULL MULTILEVEL SECURE SYSTEMS ARE IN R&D
  - LIMITED MULTILEVEL SYSTEMS ARE AVAILABLE
- COMPUTER SECURITY EVALUATION CENTER IS:
  - ADDRESSING TECHNICAL / PROCEDURAL SOLUTIONS
  - ESTABLISHING STANDARDS
  - EVALUATING SYSTEMS
  - PERFORMING R&D

1D1329, PENTAGON, D87504.3 • 17 OCT 83

OBSERVATIONS

- DOD COMPUTERS CONTAINING CLASSIFIED DATA ARE PROTECTED
  - ELECTRONICALLY - PHYSICALLY - CLEARED PERSONNEL
- THE NUMEROUS UNCLASSIFIED DOD COMPUTER SYSTEMS ARE MUCH MORE VULNERABLE TO HOSTILE EXPLOITATION
- FULL MULTILEVEL SECURE SYSTEMS ARE IN R&D
  - LIMITED MULTILEVEL SYSTEMS ARE AVAILABLE
- COMPUTER SECURITY EVALUATION CENTER IS:
  - ADDRESSING TECHNICAL/PROCEDURAL SOLUTIONS
  - ESTABLISHING STANDARDS
  - EVALUATING SYSTEMS
  - PERFORMING R&D
- **LONG-TERM SOLUTIONS WILL RELY HEAVILY ON INDUSTRY INITIATIVES**
- **GREATEST RISK IS PEOPLE**

NATIONAL TELECOMMUNICATIONS
AND
INFORMATION SYSTEMS SECURITY
COMMITTEE

EXAMINATION OF NATIONAL SECURITY DECISION DIRECTIVE 145
NATIONAL POLICY ON TELECOMMUNICATIONS
AND AUTOMATED INFORMATION SYSTEMS SECURITY

STATEMENT BY

DONALD C. LATHAM

ASSISTANT SECRETARY OF DEFENSE
COMMAND, CONTROL, COMMUNICATIONS, AND INTELLIGENCE

AND

CHAIRMAN
NATIONAL TELECOMMUNICATIONS AND INFORMATION SYSTEMS SECURITY
COMMITTEE

BEFORE THE
SUBCOMMITTEE
ON
TRANSPORTATION, AVIATION AND MATERIALS

COMMITTEE ON SCIENCE AND TECHNOLOGY
UNITED STATES HOUSE OF REPRESENTATIVES

JUNE 27, 1985

Mr. Chairman and Members of the Subcommittee:

Thank you for this opportunity to testify regarding the general climate that led to National Security Decision Directive (NSDD) 145, "National Policy on Telecommunications and Automated Information Systems Security," and the objectives, structure, responsibilities, and accomplishments arising from the NSDD, as well as the likely impact on institutions and agencies not normally considered a part of the national security establishment.

Our modern world is heavily dependent on telecommunications and data processing. Every day each of us uses telecommunications or data processing facilities in a myriad of ways. There are almost daily announcements of the latest developments in these fields. Yet, for all our dependence on these disciplines, for all the money spent on developing new technology, and for all the trust we put in these systems with information about our nation's most vital secrets, the 1982-1983 Biennial Report on the Status of communications security in the Federal Government proclaimed that it is in a perilous state! Virtually every aspect of Government and private information is readily available to our adversaries - unfriendly governments and international terrorist organizations alike are finding easy pickings in the flood of unprotected telecommunications and automated data processing information afloat in this country.

This report recommended that a number of objectives be adopted to protect sensitive government information. It called for:

- Improved planning, development and production to deliver more communications security (COMSEC) equipment sooner and at lower cost

- Reorganizing and refocusing the COMSEC policy-making structure to facilitate requirements definition, prioritization, and funding

- A substantial increase in funding for COMSEC

- A significant near-term increase in the availability of secure telephones throughout the government.

- Increased efforts to secure computerized data networks and associated office automation equipment

Communications security was first declared a national responsibility by President Truman in the 1952 Presidential Directive that established the National Security Agency. He directed that the National Security Council establish a United States Communications Security Board (USCSB) to be responsible for integrating COMSEC policies and procedures throughout the Government. He also established that the Secretary of Defense would act as the Executive Agent for communications security for the entire Government, and that the Director, NSA (DIRNSA), would act for the Secretary of Defense in implementing these COMSEC responsibilities.

In 19/7, recognizing a need to strengthen our posture against the hostile threat to government communications across the board, President Carter issued Presidential Directive Number 24, entitled "Telecommunications Protection Policy," which modified the Truman structure and split COMSEC responsibilities between the Secretaries of Defense and Commerce. The National Communications Security Directive, creating the National Communications Security Committee (NCSC), was issued by the Secretary of Defense in 1979 to complete the Carter structure. The National COMSEC Directive reaffirmed the responsibilities of the Executive Agent and the DIRNSA.

Although the NCSC promulgated a dozen statements of Policy and more than fifty Instructions and Information Memoranda, the increasingly challenging threat to our telecommunications required an even more broad-based approach involving the civil and military sectors of government, and the private sector as well. National Security Decision Directive (NSDD) 145, the National Policy on Telecommunications and Automated Information Systems Security, was signed by President Reagan on 17 September 1984. This Directive confirms the basic tenet of the entire communications security process as it applies to both telecommunications security and information systems security, namely that COMSEC is a national responsibility. NSDD 145 directs a reorganization and refocusing of the national COMSEC and computer security policy-making structures. Thus, NSDD 145 is a direct response to one of the objectives of the 1982-1983 Biennial Report.

NSDD 145 provides for the safeguarding from hostile exploitation of systems which process or communicate sensitive information. That information may be classified national security information or other sensitive, but unclassified, Government or Government-derived information, the loss of which could adversely affect the national security interest. The NSDD also directs the Government to encourage, advise, and, where appropriate, to assist the private sector to identify systems which handle sensitive non-government information, and to evaluate their vulnerability and suggest measures for their protection.

The Systems Security Steering Group is chaired by the President's National Security Advisor, and its members are the Secretary of Defense, the Secretary of the Treasury, the Secretary of State, the Director of Central Intelligence, the Attorney General, and the Director of the Office of Management and Budget. The National Manager for Telecommunications and Automated Information Systems Security (Director, NSA) is the Executive Secretary. The Steering Group is expected to take an active role in carrying out the National Policy on Telecommunications and Automated Information Systems Security, and will meet at least twice a year. During the first meeting each year, the Steering Group will review the security status of those telecommunications and automated information systems that handle classified or sensitive Government or Government-derived information and will develop guidance for program and budget development. At the second meeting they will review the programs and budgets assembled by the National Manager, and will formulate recommendations to pass to the Office of Management and Budget (OMB) for use during OMB budget reviews.

We expect that the cabinet-level membership, and the President's National Security Advisor as Chairman of the Steering Group, will ensure that programming and budgeting for telecommunications security and automated information systems security receive the wide high-level Executive Department exposure needed to get the necessary resources (another of the objectives expressed in the Biennial Report). Under the previous system, COMSEC and COMPUSEC (Computer Security) were not programmed and budgeted with a national perspective; and those agencies which are not primarily in the national security sector had little role in the decision making.

The National Telecommunications and Information Systems Security Committee (NTISSC) is the operating level interagency organization subordinate to the Systems Security Steering Group. In addition to the three military departments, the NTISSC membership includes the Joint Chiefs of Staff and the Marine Corps as voting members, as well as a broad representation among other DoD and civil agencies. The Committee is comprised of senior representatives who are decision-makers for twenty-one Government departments, agencies and the military services. There are also seven non-voting observer representatives. I am the Chairman of the NTISSC.

The NTISSC has an impressive array of responsibilities and has established a National Issuance System for promulgating operating policies, directives, instructions and guidance. This system will be maintained by the NTISSC Executive Secretariat as the NTISS Issuance System. It will include the Policy statements, Instructions and Advisory Memoranda developed by the former NCSC until they are replaced or updated by the NTISSC.

The NTISSC Subcommittee on Telecommunications Security (STS) currently is defining information considered to be unclassified, but sensitive. The STS will soon have a draft national policy for consideration. Adoption of the national policy will initiate specific steps within the departments and agencies of the government. This policy applies only to that portion of the life of information during which it is being electronically processed or transmitted. If it is not protected during this processing or transmission, it is vulnerable to unauthorized and undetected interception and exploitation by parties unknown to authorized users of the information. This policy in no way applies to the release of sensitive, but unclassified information directly by departments and agencies of the government to authorized and intended recipients, which is a departmental prerogative. These standards apply only to protection from unauthorized access during electronic processing or transmission.

The NTISSC adopted NTISS Directive 900, Governing Procedures of the NTISSC, and NTISS Policy 1, "National Policy on Application of Communications Security to U.S. Civil and Commercial Space Systems." Adoption of the national policy on COMSEC of civil and commercial space systems set standards for telecommunications systems which may be used for government or government contractor communications. The government will encourage the application of these standards to all commercial systems. A directive establishing the NTISS Issuance System is due for vote soon, and a directive on COMSEC monitoring is in the review process. Policy issuances on the Protection of sensitive Information and on Access to U.S. Supercomputers also are under review. An NTISS Instruction on Controlled Cryptographic Items has been approved, and Instructions on Classification Guidelines, Computer Criteria, Safeguarding and Control of DES Equipment and Unclassified COMSEC, Operational Doctrine for the Fleet Broadcast System, COMSEC Utility Program, Global Positioning System User Terminals, and a Systems Security Material Fund are in drafting or under review. The NTISSC also has acted on requests for the release of cryptographic equipments to the Federal Republic of Germany, the Netherlands, and NATO.

Under Executive Order 12333, the Secretary of Defense is Executive Agent of the Government for COMSEC. NSDD 145 expands the authorities of the Secretary of Defense as the Executive Agent of the Government for COMSEC to include automated information systems security. The Directive also establishes a national manager as the operating arm of the Executive Agent. The Director, NSA (DIRNSA) is the National Manager. This consolidation of computer security and communications security under a single Government Manger is in line with the trend in technology which blurs the distinction between telecommunications systems and automated information systems. This trend already has led many organizations to establish a single senior manager responsible for both fields. The military services, civil departments and agencies of the Government, and our NATO allies all reflect this trend. The Secretary of Defense as Executive AGent and the Director, NSA, as National Manager respond to the direction of the Systems Security Steering Group and to the NTISSC, who formulate policy, set objectives, and establish priorities.

Since National Security Decision Directive 145 was signed in September last year, many efforts have been underway to realize its direction. One of these is in response to the requirement that the NTISSC submit an annual evaluation of the status of National Telecommunications and Automated Information Systems Security to the Systems Security Steering Group. This will replace the old Biennial Report which was last submitted in February 1984.

The first Annual Report provides a measure of how well we've done in meeting the objectives of the Biennial Report, spells out the challenges we still face. and recommends our objectives for the coming year.

The chairmen of the NTISSC subcommittees for Telecommunications Systems Security and Automated Information Systems Security were tasked to provide separate evaluations dealing with their respective subject areas. The Executive Secretariat consolidated the two subcommittee evaluations and submitted the consolidated report to the NTISSC for review. The evaluation is now under review by the NTISSC membership. We anticipate submission to the Chairman of the Systems Security Group before the end of this month.

All of you are users of our telecommunications and automated information systems. Most of you will, at one time or another, have occasion to discuss sensitive information, whether it be classified national security information, or sensitive, but unclassified Government or non-Government information. Regardless of which category it falls in, it needs protection from those who would use it to the disadvantage of our country. It is our goal to make low-cost, effective protection equipment available as widely as possible. However, the only way security can be effective is if everyone uses protection whenever there is a question of sensitivity in the data being exchanged, whatever the means of transmission.

National Security Decision Directive 145, in establishing the new National Policy on Telecommunications and Automated Information Systems Security, is refocusing our national COMSEC and COMPUSEC policy-making structure to recognize the changing nature of telecommunications and automated information systems. As these technologies change, we must stay abreast of the changing concerns and relationships that emerge as a result. With the National Authority vested in the NTISS System by the Presidential signature on National Security Decision Directive 145, and with broad participation within the civil and military sectors of the government (and we hope the private sector as well), we have high hopes of protecting a significant portion of the data now being lost to our adversaries through the telecommunications and automated information systems upon which we are all so heavily dependent.

Mr. Chairman, this concludes my prepared testimony. I will be pleased to answer any questions that you or the Subcommittee may have.

Mr. GLICKMAN. We will have our next two witnesses go together. Walter Deeley, Deputy Director for Communications Security; and Robert Brotzman, Director, DOD Computer Security Center. Dr. Brotzman has been, of course, before this committee before on, I think, the same subject, generally.

So, we are delighted to have you both here today, and you may follow Secretary Latham's lead and summarize, or you may read your statement, as you deem appropriate.

STATEMENTS OF WALTER G. DEELEY, DEPUTY DIRECTOR FOR COMMUNICATIONS SECURITY; AND ROBERT L. BROTZMAN, DIRECTOR, DOD COMPUTER SECURITY CENTER, NATIONAL SECURITY AGENCY, FORT MEADE, MD

Mr. DEELEY. I am Mr. Deeley. I prepared two papers. One is verbal testimony, another written testimony, because of the length of what I would like to put before this committee.

Mr. GLICKMAN. That is fine. Your entire written testimony will appear in the record, so you may——

Mr. DEELEY. And on the basis of some remarks you made in your opening statement, an indication of something that I think is far from the truth, I am also going to make an extemporaneous statement, if you will.

Mr. GLICKMAN. Sure.

Mr. DEELEY. And perhaps even before I begin my verbal testimony. The statement has been made that—and in fact, you made it, sir—that NSA is an arm of the military.

I say, the statement has been made, and you made it, that NSA is an arm of the military, and it has later been said that NSA is military-related. I would like to set the record straight on that.

Mr. GLICKMAN. OK.

Mr. DEELEY. NSA is truly a national agency. It was ordained by President Truman in 1952, with a document called, "National Security Council Intelligence Directive No. 6." NSA has taken that to heart ever since those days. It really regards itself as an agency that has a national interest as a responsibility, as a mission.

It is predominantly military in terms of the SIGINT information that it produces, and has been so for many, many years. That is because our biggest customer, if you will, is the military.

But it has also provided support to the civilian side of government, ever since its inception, and it sends today product to the Department of Commerce and the Department of the Treasury, and all of the parts of Government, in terms of that part of its mission. NSA has two missions.

It has signals intelligence—NSA is often characterized in that regard, not taking into account the other two missions, namely communications security, which was, again, a part of President Truman's Directive, and computer security.

NSA, for all practical purposes, is in the Department of Defense for rations and quarters. It really speaks to the national requirements. It is under the executive agency of the Secretary of Defense. It is not a defense agency, per se, it is a national agency.

Mr. GLICKMAN. Who does the Director of NSA report to?

Mr. **Deeley**. To the Secretary of Defense directly as the executive agent of the Government, not as the Secretary of Defense. So, NSA is beholden to the Government at large in performance of its mission, both SIGINT and communications and computer security.

I want that on the record, that it is truly a national agency. It was chartered that way, it answers to the Secretary of Defense directly in his role as the executive agent of the Government's, the signals intelligence and communications——

Mr. **Glickman**. I am sorry to interrupt you, but you made remarks to my extemporaneous remarks, so I am going to do it to you.

It is my understanding that NSA does not have a formal legal charter. Is that correct?

Mr. **Deeley**. Well, in a sense, that can be construed that way. It does have public laws that underwrite its mission. There is Public Law 86-36, which does,[1] indeed, charter NSA, not in the same sense as the National Security Council Intelligence Directive, and the executive order do. NSA has gone through a metamorphosis, if you will, since President Truman established it.

There have been a series of National Security Council intelligence directives which changed its mission, which enlarged it, which construed it. In 1958, for example, we picked up the responsibility for electronics intelligence. It used to have only communications intelligence.

So it has metamorphosized, if you will, over that period of time. It does not have charter legislation in terms of identifying precisely how it fits in the Government.

When Bobby Inman was Director of NSA, there was an attempt at that time to have charter legislation, and for some reason, it went away. I suppose there could be charter legislation, but certainly, its responsibilities, mission, constraints, and everything else are on the books, in official national documents.

Mr. **Glickman**. Do you think it would be helpful to have——

Mr. **Deeley**. As a personal opinion, I do so believe that it would be helpful to have charter legislation for the National Security Agency.

Mr. **Glickman**. Thank you.

You may proceed.

Mr. **Deeley**. Mr. Chairman, members of the subcommittee, thank you for this opportunity to testify regarding a subject which I submit is one of the most important we have to address in our time: The state of security of our Nation's information and telecommunications systems.

You have asked that NSA address many of the subjects related to the National Security Decision Directive 145, and I am prepared to do that, and propose the following:

I have submitted written testimony which covers the general climate of the Nation's information and telecommunications situation which led to NSDD 145. The overall structure and responsibilities of 145, any number of essential communications security initiatives that have been or must be undertaken if we are to be successful in providing an acceptable telecommunications security posture for the United States.

---

[1] Line 889: insert after "There is Public Law 86-36, which does," the phrase, "insofar as it provides authority for certain personnel practices and related reponsibilities"

I will preface my remarks by telling you that I view the subject of communications security from a unique perspective. Before I took my present position as the operating official in charge of communications security for the United States, I spent 35 years of my life engaged in signals intelligence against other countries.

Viewing my new mission against the old frightens me. The United States is in jeopardy because it does poorly in protecting its vital communications.

Should we protect our information? Our society is open, and we are a people who cherish our freedoms. We are naturally gregarious and given to trust. It is not in our nature to trust a government given to secrecy, as you will hear later in the testimony.

This Government is not given to secrecy. However, if we wish to maintain the society that we have, and continue the freedoms we fought so hard and so long to obtain, we must deny to those who would harm us the information which enables them to do so.

We have suffered egregiously in the last few decades. Traitors amongst us will sell our very secrets which preserve our Nation for dollars, not ideals.

Under oath, I will tell you that traitors have provided cryptologic information which has enabled the Soviet Union to know many of our most vital secrets. We may pay dearly for this in the future.

But while these traitors toy with our destiny for a few dollars, we give the other side, daily, a continuous flow of vital information which tilts the balance inexorably in their favor.

The damage accrues from their continuous intercept and exploitation of our unprotected communications, and periodic exploitation of protected communications through the provision of cryptologic information to the other side, either by traitors selling secrets or putting cryptology in the public domain.

The damage to the Nation is growing dramatically as we rapidly transition into the information age. The information explosion now upon us is exacerbating this problem by orders of magnitude.

National will, this was brought up during Mr. Latham's discussion. Securing our communications is not an easy task. First and most important, it will take the will to do so. We do now have this yet, as a Nation.

Some of us believe we have a right to all information. It is a freedom. Others would challenge the Government's right to choose the information to be denied the public and our adversaries.

While the debate never ceases, neither does the information flow. As we sit here now, the Soviets in Moscow are on line, by telephone, into the largest data base in the United States. We must stop the debate, decide what needs to be protected, and do so.

It is the Government's mission to protect our society. We must perform this mission. There are checks and balances to keep the Government honest. One of those resides here in the Congress.

Second, securing our communications costs money, and like insurance, you may not realize the benefits immediately and tangibly, so it may not rank with tanks and guns and airplanes or new highways and bridges in your immediate priorities.

It may just be on or just below your budget cut line. I believe that costs of security can be borne easily if we make COMSEC, communications security, ubiquitous. Spread it throughout the land. Give everyone who has a right to privacy the means to privacy. The effects will greatly benefit the national interest, and the public.

Until recently, the Government was paying tens of thousands of dollars for a single secure telephone. Soon, it will pay less than $2,000. Because of the leverage of large-scale industrial production, we will make millions of units instead of thousands.

The Government, defense contractors and the public sector will pay the price for security or privacy if the cost is reasonable. This approach can be expanded to the world of data and information security.

I would estimate as a rule of thumb that this Nation can protect its communications for about 5 percent or less of their cost, but you must want to do so. As a Nation so far, we have not made this commitment, we have spent far less than 1 percent, and we are or our progency may bear the cost, loss of our freedom.

Third, communications security is a national problem, not just another duty of managers in and out of Government. Today, it is almost a function of personality. Those who are aware of the vulnerabilities and who are responsible provide for protection.

The great majority do not. There is no accountability for those who do not. Until NSDD 145, there was no national charter with anyone in charge. There are some today who say that it is but a piece of paper with no force of law or executive mandate.

We may still have no one in charge. Who would tell the Secretary of the Department, or the Chief of Staff of a Military Service, that they have communications that must be protected? And once told, who would ensure that they did it?

How does one do this? The fulfillment of responsibility in this regard almost surely evolves from the second problem: The cost of security.

Public sector: The question is asked, Does the public sector want security? I maintain that it does, if it can afford it. When I was a young man, a number of families shared the same party telephone line, and some people knew everyone's business on the line. No one liked it except those who listened.

Economies of scale have returned our rights of privacy. I believe today that many millions of dollars are being lost our business and industry through interception of their communications.

It is my intent to alert Fortune 1000 companies of their vulnerabilities. Foreign countries intercept our industrial, commercial and banking communications for their economic advantage.

It is not in our national interest to allow others to exploit us economically through intercept and exploitation of our communications. Ultimately, I believe the insurance companies will want it stopped.

And I will make an aside here, it is the belief of the past-Secretary of the Treasury, and I think it is a well-founded belief, based on a good deal of information, that the Soviets exploited us in the grain deals to their economic advantage.

They had a great deal of information, and they were able to use it against us, economically.

Does the Government have a responsibility to the private sector? I maintain that it does. First, I will assert that cryptology, like nuclear weaponry, is Government business first and foremost.

Cryptology, the science of codes and cyphers, is the only way we can protect our vital national security communications. There is an application of higher mathematics that must be kept secret if we do not want our adversaries to exploit our codes and cyphers.

Already, too much has been bandied in public domain by well-intentioned academe, and public cryptographers, and by some who would engage for profit, even though it might result in harming the Government's codes and cyphers, and aid the exploitation of our Nation's most vital secrets.

It is time to put the genie back in the bottle for the good of our society. The Government can and should provide cryptology on a controlled basis to industry for use by the public sector. It has already undertaken to do so.

Industry may apply it in a proprietary way. The Government will certify it when it meets standards, as the Government did with the data encryption standard.

Thus, like the Food and Drug Administration's certification of pharmaceuticals, NSA will certify the implementation of its cryptologics as it does now for the Government use.

The cryptologics and variations of them can be used in the public sector. Both Government and the public benefit from widespread use. Within the terms of NSDD 145, NSA has initiated a number of programs to imbed security in the communications which would be protected or to otherwise bring down the price of security and make it available.

These programs are described in the written testimony. Our experience is that industry is turned on by these initiatives because there is a market and a profit for them, and the Government is willing to help.

We have begun a program to determine the threat to and assess the vulnerabilities of our communications to guide the process of securing them. This information will be made available to all who need it, as described in the written testimony.

We still do not have an efficient and effective funding mechanism for programming and budgeting communications security resources within the Government. The current system is described and the recommendation is made in the testimony.

Finally, there is a serious threat from foreign-owned, controlled or dominated companies selling their cryptology in the United States. Legislation is required to ensure that the Government and the public sector are not harmed.

The problem is described and recommendations are made in the written testimony.

I want to thank you for the opportunity to alert you to what I consider a serious threat. I hope that what I have said and what you have read will stimulate your subcommittee to do what it can to bring about the essential changes for placing our communications security posture where it must be for the good of the Nation.

I am convinced of the need and committed to the challenge. I will address any questions.

Mr. **Glickman**. Thank you, Mr. Deeley.

I think we will go to Dr. Brotzman before I have questions. I would like to note, for the record, however, your very distinguished career in the Government, which speaks for itself. But I think that you are example of a public servant that has certainly given his career to the—what you to believe in the best interest of your country, and have done so for a very long time.

And we may have some disagreements on specifics, but I think that your credibility here as a witness is unquestioned.

Mr. **Deeley**. Thank you very much.

Mr. **Glickman**. Dr. Brotzman?

Mr. **Brotzman**. Thank you, Mr. Chairman.

I serve as the Director of the Department of Defense Computer Security Center, and also as the chairman of the Subcommittee on Automated Information Systems Security, as mentioned by Mr. Latham.

Thank you for this opportunity to describe some of the activities of the center, and of the subcommittee, which support the National Security Decision Directive No. 145.

Several days ago, the full text of my testimony was delivered to the staff, and I would like to present just a short synopsis of that.

The computer is today's prime force for change. It is reshaping our lives in the second half of this century, just as the automobile and the airplane did in the first half.

The clock moves only forward, and we cannot turn away from this new revolution, the computer revolution, nor do we want to do so. It serves us very well. The computer is assuming our burdens on tasks that are tedious, and giving us the power to break through barriers that once seemed insurmountable.

To enable this immensely talented servant to do its job, we have entrusted it with our knowledge base. The computer has become the custodian of our defense secrets, of our financial accounts, scientific data, proprietary information, and personal records.

Nearly all information that matters that is not already stored in some computer soon will be. We have expended enormous resources to teach the computers to manipulate, to retrieve, and more recently, to make inferences about the information generated or fed to them.

Our success has been monumental and building a momentum that ensures that future success will be more rapid and more profound.

But our success, like our effort, has been largely limited to increasing the utility of the computer. We have taught it much about how to use its knowledge base, but very little about how to protect that base from improper use.

The jeopardy that insecure computer systems imposes to our security, our economy, and our personal freedom will increase in proportion to our dependence on those systems. That dependence is accelerating.

Federal programs ranging from national defense, intelligence, space, air traffic control, health, social welfare, and financial activities rely on computer support. Computers are essential components in our weapons systems.

Most major governmental activities could not meet their mission objectives without the use of computers. Many of the critical activities within the private sector have a similar dependence.

The computer industry of the United States is $140 billion a year juggernaut growing at a rate of between 16 and 20 percent per annum, and proceeding relentlessly down a very risky road.

We seek to divert that rambling giant onto a different path, a path that includes good security features right along with high utility. To succeed, we must obtain extraordinary leverage from every dollar, because the industry to be altered dwarfs the resources we have committed to effect that alteration.

We are in a race where holding our own would be a remarkable achievement, but failure to close the existing gap cannot long remain an acceptable option.

The inherent ability of current computer systems to protect themselves or their data from abuse is appallingly low. Treatment is available right now which can improve their ability to function securely, but nursing systems that were born weak is only a stop gap, and not a solution.

To reduce our risks substantially, we need to develop and apply methodology that will enable us to create systems with solid security features designed in from the beginning.

In the 9 months since the NSDD was signed, a number of initiatives, both within the structure of the National Telecommunications and Information Systems Security Committee and within the Computer Security Center, have been undertaken toward implementing the structure, fulfilling the objectives, and carrying out the policies of that document.

NSDD 145 extended the responsibilities of the Computer Security Center to include the entire Federal Government, rather than just the Department of Defense. It not only expanded the scope of the center, it changed the nature of our clientele.

Most civil agencies are less aware of their computer security needs than are the agencies and departments of the Department of Defense. To the extent that they do recognize these needs, they apparently perceive them as somewhat different from those within Defense.

To service this new community, we have to raise their awareness, gain an understanding of their computer security concerns, and determine which of their needs are truly unique and which have common threads.

We do not have all the answers for the problems of the civil sector of Government, and if we did, those answers could be applied effectively only if the people concerned recognized them as valid. There will be no salvation in a forced conversion.

The threat imposed by insecure systems is one that must be addressed. It isn't just a Department of Defense problem, although the threat to our security is paramount. And it isn't just a Government problem. It looms over virtually every aspect of our lives, collectively and individually, public and private.

There are no panaceas, but there are steps that can be taken to reduce that danger.

The structure created by the NSDD has raised the level and broadened the scope of attention given to computer security, and that is an important prerequisite to dealing with the problem.

Within the center, we have charted a course which we believe to be responsive to the task set before us. We are aggressively pursuing initiatives that address both current and long-term future needs. The actions we are taking come with no guarantees. But I believe that the failure to act does carry a guarantee, and that is a guarantee of a major disaster.

I am grateful that the committee also views these problems as serious and is taking the time to examine them. With your support, we believe our chances of staving off a disaster are greatly improved.

There will be enormous difficulty in providing adequate protection to the Nation's information base and the equipment that processes that information.

If we do it and do it well, we will survive as an information-based and open society. And that is well worth doing.

Thank you, Mr. Chairman.

Mr. **Glickman**. Thank you, Dr. Brotzman, and your written testimony is very good. All the testimony that is presented today, I would say, is thoughtful testimony. Sometimes when you hold these hearings, there is a tendency to get what I refer to as insipid junk, and that is not the case today, and I appreciate the fact that you thought these things through.

I would like to ask Mr. Deeley, in the statement of the American Civil Liberties Union, they will be testifying after you, and I am going to read you just one-half of a sentence on page 2, and I want you to comment on it.

They say, "We read this directive NSDD 145—" it is on the bottom of page 2 of their statement, if you have got it there——

Mr. **Deeley**. This is Berman's?

Mr. **Glickman**. Mr. Berman's statement. You will get one right here. I just want to read this through with you, and then I want to you to respond. It is about five lines down.

> We read NSDD 145 and its designation of the Director of NSA as the National Manager for Telecommunications and Automated Information Systems Security as mandating an unprecedented, unwise, and uncheckable primacy of the Nation's national security apparatus in information policy, an area where the balanced consideration of values other than security is of paramount importance to our system of government.

Now, I wonder if you might respond to that?

Mr. **Deeley**. Yes, I would very much like to respond to it.

NSA is a technical agency, by and large. It is schooled in developing and designing cryptologic algorithms, to process information. It is designed to produce key, which we hope is the best in the world, to protect with those algorithms our Nation's information.

On the other side of the house, it uses the same kind of expertise to read or attempt to read other people's communications who would harm us. It is basically a technical agency.

It tries to take and provide the very best protective mechanisms for our country to use to protect our own information, and at the same time, it attempts to read the communications of other countries who we believe would harm us.

But it serves at the direction of the Government. What drives NSA are the requirements of people. It is a service organization, by and large. People come to us and say, "We wish to protect our communications. What can you do to help us?"

And we try to identify what their specific needs are, and produce things which will protect their communications. On the other hand, the Department of State will come to us and say, "We are concerned about what such and such a country might want to do to some of our citizens. Can you provide information to us in advance that will help protect those citizens?" And we try to do that on the other side of our house.

But we are not, if you will, a supersecret agency that tries to run over everybody, doing our thing. We respond to written requirements and only written requirements. We have now, since the Nixon era, an effective general counsel office that makes sure that everything we do is within the letter of the law.

So, you know, there seems to be a tendency by some people to suspect NSA as being an insidious mechanism within the Government trying to read everybody's mail and that kind of thing, and that is not so.

The people that populate NSA are all Americans, and in fact, I tell you, they are probably a better cut of Americans than what one might normally find in an organization, because they have to go through a very, very careful screening process.

Their loyalty is tested day in and day out. They have to submit to lifestyle polygraphs, which I find abhorrent as an individual. I think a polygraph is an insult to a man's dignity. But you have to give up a right in order to serve in a position where you are placed in the national trust, where you hold a nation's most vital secrets.

To look at NSA as being some insidious mechanism within Government, that is trying to do our Nation in, trying to read its own citizens' communications, or trying to do things wrong or harmful to the Government, is just wrong. It is bad.

Mr. **Glickman**. Well, you know, some people have said over the years that NSA does the dirty work prescribed to it by other agencies of Government.

Mr. **Deeley**. That is not so. NSA has many, many times told an organization within the Government that what it wishes NSA to provide is unlawful and it will not do so. We have been asked to withhold product to protect particular interests. We have never done so.

We operate absolutely within the law, and I think one of the best things that has ever happened to this country, is the fact of the establishment of the House Committee on Intelligence and the Senate Committee on Intelligence, and they have total, absolute total, scrutiny over what NSA does.

Mr. **Glickman**. OK. Let me move just to one other area, and that is, on page 6 of your testimony, you talk about once a department or agency head has chosen to spend money on telecommunications security or automated information systems security, the NSA, as national manager, prescribes or approves which Comsec or Compusec technique, system or equipment, will be used.

How is this going to work in practice?

Mr. **DEELEY**. All right, that is a very good question, and I understand it. Let me get very basic and technical. NSA is coming down into this coliseum, that is the way it is described to me, and you are going to be one of the Christians among the lions.

NSA has decided to go public where it has to go public. To protect the public sector and the private part of our country, it has got to say more than it has said in the past.

So, what I am going to talk to now is a little more public than we would have liked the situation to be. In my area, we produce cryptographic algorithms. They are very, very few in number.

We believe they are the best in the world. There are only a few people who can do this kind of work. It is really high mathematics. A person can get a Ph.D. in math out of a college or university, and it takes 8 to 10 years before he becomes good enough to know how to use a Cray XMP, how to build an algorithm, and how to produce key which the other guy can't, if you will, generate himself.

In fact, there are probably fewer than 20 cryptomathematicians in the country worthy of the name, that can produce these kinds of things. So you protect your algorithms as though they were, the family jewels.

Now, you don't want your algorithms being given to the other side, in any way, shape or form. So there is a degree of protection, given to algorithms. You wouldn't put the algorithm out there in the public sector that would protect the President's communications, you just wouldn't.

So, what you try——

Mr. **GLICKMAN**. You wouldn't give the Social Security Administration the same algorithms——

Mr. **DEELEY**. No, not at all. So, what you try to do is determine with the user, the agency that is asking you, or the organization that is asking you for help, the degree of protection which he needs for his information.

The ability of Exxon to read Amoco is one hell of a lot less than the ability of the Soviet Union, with its massive KGB SIGINT organization to read us. So, what you would give Exxon to protect itself against Amoco would be far less than you would give, say, the Strategic Air Command.

Mr. **GLICKMAN**. Well, let's say that I am the head of the Veterans' Administration, and I want to come up with a system to protect my computer that I am very worried about compensation claims that are falling through the woodwork, and there is people out there messing up the system, and I come up with a system, or I come to you and say, develop me a system.

Now, I presume that I come in either of two ways, either develop my own system, and then bring into this—to you as manager, or else ask your advice on what to do. Is that correct?

Mr. **DEELEY**. Right, and we will do both, and it is really up to the guy that has the system to decide whether he wants us to provide it for him, in which case, he will remunerate the Government, or if he wants us to give him technical advice and guidance in terms of how to do it himself.

Indeed, what we are really trying to do is get out of that world. NSA is trying to influence industry to build protective mechanisms right into the products that they sell.

And you have a question later that addresses that, and industry is turned on by that. They are doing it now.

Mr. GLICKMAN. OK, well, I am going to let—I am going to ask Mr. Nelson to ask questions. I think that I am going to ask you more questions at the end, but I do think that, going back to a question that I asked you before.

It might be helpful to you to seriously explore this idea of a national charter, because if, in fact, you are a service organization involved intelligence, cryptography, help to the private sector, that ought to be outlined, so the public and Congress knows exactly—rather than kind of—some kind of a loose, amorphous operation that has kind of evolved over a period of years.

I think that is one of the concerns that are raised by people, because you even mentioned, you know, post-Nixon, you have lawyers, you make sure that everything is——

Mr. DEELEY. Absolutely.

Mr. GLICKMAN [continuing]. Quite satisfactory. I would urge the—when you go back, you just indicate at least one Member of Congress thinks it is a good idea, and agrees with you.

Mr. DEELEY. Yes, sir.

Mr. GLICKMAN. Mr. Nelson?

Mr. NELSON. I thank you, Mr. Chairman, and I thank you for holding these hearings.

Let me ask you some questions on a little bit different situation. I had the privelege, oh, let's see, this is 1985, it was back in 1978, when I was in the State legislature, to pass the first computer crime bill in the Nation.

Florida's law has become a model, and now, some 40 States have now enacted computer crime laws. And last year, with the help of the chairman of the Criminal Justice Subcommittee here, Bill Hughes, we passed the first Federal computer crime legislation.

Now, what I want to ask you is, do you have, in your attempts in addressing this problem of computer security, one of the reasons for the Federal law was to give prosecutors the updated tools to go after the new, highly sophisticated type of criminal within the Federal sphere of jurisdiction.

Do you all have an opinion as to that law that was passed, and then I will have some followup for you.

Mr. BROTZMAN. Well, sir, my familiarity with that law is somewhat limited. In my reading of it, I formed the opinion that it put a great burden on the prosecution to prove intent, and I thought that it would be fairly hard to prosecute successfully under that law.

I was delighted to see the fact of the law far more than getting worried about the exact form of the content. I thought it put a marker down to indicate that the Federal Government was serious about that area, and was not going to tolerate the sort of things that had been going on.

Mr. NELSON. Mr. Deeley?

Mr. DEELEY. Oh, I agree with Dr. Brotzman.

Mr. NELSON. All right, well, interestingly, now, that is what I had not heard about the intent of the law being questioned. They have had two already. They have had two prosecutions under the law.

Both of them have been successful. So, I will check it from that standpoint.

Now, in the negotiations with the Senate, since the Senate had not had hearings, they were reluctant to take the part of the law that applied it to the jurisdiction of interstate commerce, and so that was stricken and that Bill Hughes and I and his subcommittee are working on right now.

Further, to make sure that the law applies to the clear jurisdiction, that is, the jurisdiction is clear in application to the use of computers for criminal purposes within the banking system, the Federal banking system.

Do you all have any comments about that, from your point of view?

Mr. BROTZMAN. I have none, sir. I would point out that not being in the law enforcement business, but mainly in the technical business, we are less concerned with the matters of how you deal with people who are doing wrong.

Mr. DEELEY. But what we are trying to do, we have been working now for some time with the Department of the Treasury to try to provide protective security measures for the electronic funds transfers, and that has been a very successful program, and we are about, I believe, to have success there in the sense of being able to protect billions of dollars of transactions in the electronic fund transfer, as between banks and the Federal Reserve and banks.

And that program is applauded by Treasury, and it has taken a great deal for us to do it, and it is not funded, it has come out of hide, but it is something that is necessary, and we have done it.

Mr. NELSON. Mr. Glickman's subcommittee had held hearings last year, and he brought in the 414's, the teenage hackers from Milwaukee, so named because of their area code. And one of them testifying, I asked him the question:

"When did you know that you had done something wrong?" Do you remember that question, Dan? "When did you know that you had done something wrong?" And he said, "When the FBI knocked on my door."

And so, if for no other reason, that incident served as a statement that, indeed, there is a problem with the use of computers for criminal purposes. That particular case, although the mental intent, the criminal intent, apparently was not there with those kids, that is called the mens rea, in order to have a crime, you really have to have that criminal intent. That wasn't there.

Nevertheless, it pointed out to us that there was a problem even without the mens rea. Those kids broke in—remember the Kettering, the Sloan Kettering Medical Center New York computer, and they actually damaged some of the records?

And that, of course, could have been disastrous, if you suddenly erased a lot of the medical history of patients that you were relying on.

Well, as a result of that hearing, Mr. Chairman, we, Mr. Hughes and I, put in that legislation, that when they go shopping around, when they go exploring around, and if there is damage that is done to a program or to the computer, then that is subject to a misdemeanor.

Now, do you have any of this kind of exploring around that is of concern to you that you might be able to use that part of the law that is a misdemeanor, and on a second offense, it would be a felony? That is under the existing law.

Does that have application for you?

Mr. **Brotzman**. Once again, sir, not being in the law enforcement business, we don't view it as a tool to be used by us.

Mr. **Nelson**. Well, certainly you are interested in seeing the security of your computers, and, when that is violated, you want to see somebody go after them, don't you?

Mr. **Brotzman**. Yes, sir, but I would characterize the problem slightly differently. It is, of course, of concern to the public at large that people would attack other people's systems, technically.

From my point of view, some of those people who are attacked might also be charged with operating attractive nuisances, which is to say that their security is so bad, it almost invites attack.

Mr. **Nelson**. I couldn't hear that last part.

Mr. **Brotzman**. That their security is so bad, that it almost invites attack.

Mr. **Deeley**. I think the point we are trying to make is, what NSA's responsibility would be would be to provide Sloan Kettering with the methods and procedures and capability to protect its data bases, to protect its computers, so that 14-year-old hackers or anybody else can't get in and do those things.

We provide the means to Sloan Kettering or to CitiCorp, and we are working with CitiCorp in terms of providing protective mechanisms for their banking traffic; we provide the means to protect. We certainly applaud the efforts to have from the Congress laws that prohibit doing the things that people do to each other, but our only purpose is to provide the means to do the protection.

So, if Sloan Kettering had come to us and said, "We think there are hackers that can get into our data base and damage our records, and that is wrong, and can you help us?" We would have said, and here is the kind of thing that you can do, and we will try to help you.

Mr. **Nelson**. Well, now, Mr. Brotzman, you are Director of the DOD Computer Security Center. Your bailiwick is specifically to make sure that DOD computers don't get violated.

Mr. **Deeley**. All computers now.

Mr. **Brotzman**. It is now a national mission, sir, with the NSDD 145 being advanced.

Mr. **Nelson**. That is terrific. And I applaud you for that effort, and so, now you have application to—you have direct mission that you can support Sloan Kettering——

Mr. **Deeley**. Right.

Mr. **Nelson** [continuing]. In other words.

Mr. **Deeley**. Right.

Mr. **Nelson**. OK.

Now, I want to urge you, you all are claiming that is not within your bailiwick, and I understand that, but it seems to me that one way of trying to keep computers secure is to make sure that everybody understands what the law is.

And if everybody understands that there is a new law, and, as you say, it sets a standard by which people now know this is an activity which will not be tolerated, you all ought to be up to snuff on that.

And that seems to me would be a useful tool to you as you are helping explain what you are trying to do to other people to let you know that you have got the full weight of the law behind you.

Mr. DEELEY. We applaud the law. We are for the law. We support it. And if Sloan Kettering doesn't have a law to go to, then it is at peril. But it also has to have the means to protect itself, and that is what we are for. The two together, if you will, the law that says certain things are wrong, and you can't do them, and the means then to provide a Sloan Kettering with the means to protect itself.

So the two go in tandem and in parallel. But as Dr. Brotzman says, we are really not in the law enforcement business.

Mr. NELSON. I want to give you just one specific example of what had happened, Mr. Chairman, and I won't take much time here, I just want to share this, because it is a classic case of where a quirk in the law could have been disastrous.

A former Federal Reserve employee, in what was known as the *Langevin* case, about 2 years ago, was employed by a brokerage house in New York City, used the password of a present Federal Reserve employee, and accessed across the telephone lines from New York City to the Federal Reserve's computer in Washington the particular program on the supply of money, M1 and M2, which obviously is very valuable information to someone who is making investments and so forth.

And of course, that is why it is kept very secure. An alert supervisor at the Federal Reserve happened to note that the computer was accessed using the password and the code of an employee who happened not to be there that day, because he was sick.

And so, he immediately checked it out, traced it down, the guy 'fessed up. He was prosecuted under the wire fraud statute, because he was using interstate telephone lines. Had he made that call not from New York City, but from Washington, DC, into the Federal Reserve computer, the max penalty would have been $100 fine.

Now, there is a dramatic example of why expanding that law into the Federal jurisdiction was needed. We had had testimony from a lot of prosecutors, from the FBI, from various other law enforcement agencies that this was going to be helpful.

So I take this time just to help educate you and encourage you to, where knowledge of that law will help you in your efforts, go on and use it.

Thank you, Mr. Chairman.

Mr. GLICKMAN. Thank you, Mr. Nelson. And, to a large extent, the ability of law enforcement agencies to deal with this problem on the civilian side is due to your efforts.

I am just going to ask you, basically, one more question, because Mr. Brooks of Texas has come in, and he will be testifying next.

I am going to introduce a bill today that will mandate that all Federal civilian agencies establish computer security training programs within their agencies, and also will amplify the National Bureau of Standards' program to provide assistance and help, training, personnel, and whatever, that they currently do within their—you know, they have a computer security function within there—to provide that help to existing Federal agencies.

Would you view that legislation in the abstract way that I have described it as consistent or inconsistent with the committee that NSA is the manager of?

Mr. **Brotzman**. As described, Mr. Chairman, I see no inconsistency. One of the policies being followed in implementing NSDD 145 is to use those organizations and skills in government now existing, rather than reinventing organizations to do things.

We are trying within the national structure to use the skills of NBS currently, within the NSDD 145 structure.

Mr. **Glickman**. Mr. Deeley?

Mr. **Deeley**. I would say there is a bit of a difference. I think one of the reasons why NBS, was not able to take on the massive tasks that it had in PD-24, to do the civilian side of government, is because of the lack of resources and the lack of expertise that it had.

With regard to standards, it is probably the best in the world. But in terms of training across the whole rubric of computer security, in terms of training people to adopt measures to protect local area nets, to protect the cryptologics, that would be used in the computer security, they really do not have the expertise.

You would have to start almost from scratch with NBS to—in the standards world, they absolutely can do it. Outside the standards world, you would have to capitalize them, and it would be a rather large capitalization, and I guess it would be sort of duplicative of what we are trying to build now in the National Computer Security Center.

So I would say, sure, every Department and Agency ought to have a training program. With regard to standards, it definitely ought to be within the National Bureau of Standards, but across the whole realm of computer security procedure and practice, you ought to centralize it.

Mr. **Glickman**. OK, we thank you both for coming here today, and appreciate it very much.

Mr. **Deeley**. Thank you very much, sir.

[The prepared statements of Mr. Deeley and Mr. Brotzman follow:]

STATEMENT OF

WALTER G. DEELEY

DEPUTY DIRECTOR, COMMUNICATIONS SECURITY, NSA

AT HEARINGS

BEFORE THE

SUBCOMMITTEE ON TRANSPORTATION, AVIATION
AND MATERIALS

COMMITTEE ON SCIENCE AND TECHNOLOGY

U.S. HOUSE OF REPRESENTATIVES

JUNE 27, 1985

I. Introduction

The communications security (COMSEC) situation in this Nation is in a critical state. We have taken a number of measures to lessen the critical situation but much more needs to be done to place us in a satisfactory state. One of the actions taken was the issuance of National Security Decision Directive (NSDD) Number 145. This testimony is in response to your request for assistance in examining the general climate surrounding NSDD 145, its status and related plans and initiatives.

II. COMSEC Climate

Historically this Nation has paid too little attention to the security of its communications. Even after the obvious benefits we and our allies obtained from our intercept and exploitation of Axis communications in World War II, we have not applied the lessons to our present communications and asked "Is this happening to us now in the cold war, the economic war, the technology war?" Consequently, we started the decade of the 80's way behind. Then along came the Information Explosion, the computer revolution, the third wave. We are rapidly becoming a nation of information handlers while treating the security of information as if we were still in the industrial revolution. Without a radical and rapid change we will be so far behind by the end of the 80's that catch up will be nigh impossible.

What are the central roots of this problem? Foremost, and it can be argued that all other roots of the problem essentially follow, we have not had a "national will" for securing our communications. We have not had central leadership. Without leadership most endeavors will not flourish and U.S. COMSEC is not an exception. What we have accomplished has been the result of the efforts of the Department of Defense, NSA and the military services and a few outside the Department who are concerned.

Without a national COMSEC "will", we have not had a COMSEC advocacy sufficient to stimulate an awareness of the critical nature of the situation. Without awareness we have not had the demand for products that can lead to sufficient quantities which in turn, leads to economies of scale and then to cost effectiveness. Instead of being on the down slope of the cost curve we have been on the up spiral.

The above situation has resulted in a paltry amount of COMSEC being fielded over the past decades as a compared to the real need.

The information explosion is bringing about a somewhat heightened interest in the need for security, for example hacker publicity and the banking industry's concern about moving billions of dollars electronically. The very technology that is bringing computers into every office can also be harnessed to bring about less costly, more user-friendly COMSEC. The industry that is bringing about the information explosion is also a force that can be brought to bear on the situation. Supply side economics can be used for COMSEC just as easily as for other products.

With this as a backdrop, a course was laid out that would take advantage of these openings. First, NSDD 145 was intended to establish the national will for COMSEC and treat the lack of singular, accountable leadership. There are those that claim that NSDD 145 might not actually accomplish these aims. If in fact it does not then the very root problem is still with us and the other initiatives that will be described will be in severe jeopardy of success.

Second, an aggressive program was initiated to couple the telecommunications industry with COMSEC, to bring about a merger of their expertise and ours. It is only through an attempt to get on the crest of the information explosion will we ever have a chance of catching it and keeping up with it. The response to this program has been great. The endeavor is linked with the increasing COMSEC awareness occasioned, in large part, by a responsible and concerned press relating the problem. It is the recognition of a demand that stimulates U.S. industry to supply its energy and this demand recognition is taking place. As a rule of thumb, this nation can protect its communications for about five percent of their costs.

Third, to heighten the awareness for the need for COMSEC, to stimulate demand, and to wisely use our COMSEC resources, the National COMSEC Assessment Center has been formed. The center is responsible for providing a continuing program of assessment of the nations security needs. This includes government, defense contractor and the private sector. We have a responsibility to the private sector and it is our intent to alert companies such as the Fortune 1000 companies to their vulnerabilities.

Fourth, legislative initiatives crucial to bringing about an orderly COMSEC explosion have been undertaken. One of the "other sides of the coin" in bringing the creativity of U.S. industry into the COMSEC solution and the provision of COMSEC systems to the private sector is the need to maintain sufficient control of the cryptographic techniques so that the security of COMSEC systems themselves are not jeopardized. Government must maintain control of these cryptographic techniques if we do not want our adversaries to exploit them and the information they protect. This also means that we cannot afford to have foreign owned, controlled or dominated firms designing or manufacturing our COMSEC. Finally, to stimulate demand in the private sector we believe that appropriate financial incentives are in order. The dire need for large scale implementation of secure systems in the government and the private sector, the significant economies-of-scale and its low cost COMSEC derivatives that can be gained by a significant private sector market begs for consideration of special incentives for stimulating this market. In the face of the current tax climate, it has been proposed that legislation permitting a COMSEC tax credit for private sector be enacted.

This is a quick summary of the COMSEC climate surrounding NSDD 145 and the related initiatives to bring about a state of wide application of good, inexpensive COMSEC in this Nation. The following sections will describe the structure and responsibilities outlined in NSDD 145, identified shortcomings still resident in the process, and additional details on the related initiatives.

III. NSDD Structure and Responsibilities

National Security Decision Directive 145 is the first step in a process of expressing a national will to secure sensitive U.S. information which, in the wrong hands, would damage the National security or national interest. This section will cover what the NSDD has done in the way of establishing a policy structure and national objectives, and of some additional tasks which are urgently required.

NSDD 145 provides a cabinet-level Systems Security Steering Group to set policy and provide guidance. It provides an operating level National Telecommunications and Information Systems Security Committee (NTISSC) to prioritize objectives, provide guidance, identify systems that handle sensitive information, make recommendations to the Executive Agent, the National Manager and the Steering Group, and manage a National Issuance System. These are all positive steps.

Under Executive Order 12333, the SECRETARY OF DEFENSE IS EXECUTIVE AGENT of the Government of COMSEC. NSDD 145 expands the authorities of the Secretary of Defense as the Executive Agency of the Government for COMSEC to include automated information systems security. The Directive also established a National Manager as the operating arm of the Executive Agent. The Director, NSA is the National Manager. This consolidation of COMPUTER SECURITY and

COMMUNICATIONS SECURITY under a single Government Manager is in line with the trend in technology which blurs the distinction between telecommunications systems and automated information systems. This trend already has led many organizations to establish a single senior manager responsible for both fields. Th~~e militar~~y departments, civil departments and other agencies, and our NATO allies, all reflect this trend.

NSDD 145 mandates that, for both telecommunications security and automated information systems security, the responsibilities of the Executive Agent be carried out by the National Manager. The NSA, as National Manager, acts as the Government focal point for cryptography, telecommunications systems security and automated information systems security. The NSA's responsibilities as National Manager are wide-ranging and vital to the security of our nation's telecommunications and information systems. However, they are not to be viewed in isolation, for without the active participation and support of all elements of the Government, and that portion of the private sector which handles sensitive Government (and non-Government) information, our national and private secrets will remain exposed to any adversary. While the NSA's COMSEC authority over systems approval is clear, implementing COMSEC remains the responsibility of each department, agency, or service that uses telecommunications or automated information systems. Once a department or agency head has chosen to spend money on telecommunications security or automated information systems security, the NSA, as National

Manager, prescribes or approves which COMSEC or COMPUSEC technique, system or equipment will be used.

For the first time, in the development of the FY87 budget, the National Manager will review and assess the programs and budgets of all the department and agencies of the government (not just the military departments and certain Defense agencies). The National Manager will recommend alternatives to the Executive Agent and the Steering Group. This review and assessment by the National Manager will include not only fiscal considerations, but also will link together the vulnerability of and the threat posed to an organization's telecommunications systems, the requirements to secure those communications, and his recommendations to provide the required COMSEC. This process enables the Executive Agent and the Steering Group to review one budget proposal for telecommunications systems security which has been reviewed by the National Manager. However, NSDD 145 makes no provision for centralized budget control, except that the Steering Group will review a "consolidated" budget for telecommunications systems security. At present, the National Manager does not prepare or defend a consolidated budget; his authority is limited to reviewing and assessing individual departmental and agency input and recommending alternatives. The decision on whether to, how much to, and when to program funds for telecommunications security and/or automated information systems security is retained by the department and agencies involved.

As a consequence, when programmed COMSEC initiatives are not adequately supported in an agency's budget, or when procurement funds are not transferred to NSA in a timely manner, national requirements may not be met. Also, unit prices of COMSEC will go up, deliveries will be late, and sensitive information will go unprotected.

The mechanism described under NSDD 145 would appear to provide a national COMSEC budget, with the National Manager, the Executive Agent, and the Steering Group all reviewing the submission, and providing recommendations to the OMB, but the realities of the present budget process will probably mitigate against significant improvement in either the amount of protection provided or in the cumbersome Government COMSEC development and procurement process.

Why such pessimism? The NSDD structure still means that every department and agency (defense and civil) will continue to be controlled in their COMSEC expenditures by the overall needs of their organization. Unless it specifically requests it, the Congress will not see a Government-wide telecommunications security budget. The execution of funds appropriated for COMSEC equipment purchases will continue to require funds transfers, with all their inherent inefficiencies, even when the budgeted funds survive reprogramming for changing priorities.

An example very close to home is the COMSEC Resources Program (CRP) in the Department of Defense. It is subject to decisions concerning the total Defense Budget authority, and therefore will remain in direct competition with major Command & Control initiatives, weapons systems and other war-fighting capabilities. Even in Defense, despite acknowledgment of the critical state of our nation s communications security, current Defense fiscal guidance shows a reduction in the NSA portion of the CRP funding profile in levels below FY86 levels in every year of the FY87-91 period. With this situation in the Department of Defense, which is inherently more sensitive to communications security needs than are the other departments and agencies whose primary missions may be perceived as only indirectly related to national security, we cannot be optimistic about the prospects for an improvement.

The procedures for actually spending the funds appropriated by Congress were not changed as a result of NSDD 145. With the exception of direct purchases under the Authorized COMSEC Vendor Program and the Commercial COMSEC Endorsement Program (addressed later) the acquisition of COMSEC equipment continues in the traditional way, with NSA serving as the central procurement authority, but subject to MIPR and fund transfer delays and quantity changes working against implementation of production strategies that could reduce the time and cost of delivering expensive and complex hardware.

The National Manager's proposal for centralized budget control and authority is intended to bring order to a fragmented budget development and execution process. Its essential elements involve how and what the Congress reviews, and what and to whom the Congress authorizes and appropriates funds. It calls for the development (under NSDD 145 procedures) and presentation to Congress of a single Government-wide telecommunications systems security budget instead of the fragments now contained in a large number of departments and agency budget proposals. The process proposes disengagement from the traditional departmental budget authority, review by a few concerned Congressional committees, and appropriation of funds to the National Manager (NSA) or to the community as appropriate. It provides for the retention, where required, of centralized acquisition by NSA, but eliminates the bureaucratically burdened need to MIPR or transfer funds. It places a large measure of responsibility for both determining the make-up of the telecommunications security budget and wise budget execution on the agency that has COMSEC as a primary mission.

This program/budget process, which is termed "National Funding," could stem from the implementation of NSDD 145. It is obviously a departure from the previous method of funding COMSEC within the Government. Despite the substantial efforts of the National Manager to promote the "National Funding" concept, it was not accepted by key organizations in the NSDD 145 coordination Process.

The House Permanent Select Committee on Intelligence has recommended the executive branch consider that all communications security budgets be consolidated under NSA effective with Fiscal Year 1987. They view a consolidated National Telecommunications Security Program as the only way to establish a coherent and focused approach to communications security. We agree that this important aspect of our nation s security cannot be left to piecemeal management, but must be made a coherent and focused effort administered by the National Manager. Legislation in this regard would help to improve the national COMSEC posture.

IV. Industry Partnership

It became very clear early on that the only way to have COMSEC keep pace with the telecommunications explosion was to join it. COMSEC had to get on the crest of the wave. To accomplish this the Government has to join forces with U.S. industry and merge the relative expertise and objectives. Two significant programs have already evolved from this effort - The Authorized COMSEC Vendor Program and the Commercial COMSEC Endorsement Program (CCEP).

The Authorized COMSEC Vendor Program was a direct result of the initiative to respond to National COMSEC Instruction 6002. This requires government to specify the need for COMSEC measures as a part of all classified and sensitive contracts in a concerted effort to stem the loss of vital information resulting from intercept of defense industry communications. Government contractors can acquire the COMSEC directly and charge the costs to government in accordance with procurement regulations like other contract related security costs. NSA has authorized (via a memorandum of understanding) certain current COMSEC contractors to market directly to other government contractors, as well as to the government, the COMSEC products they are producing for NSA.

The Commercial COMSEC Endorsement Program is an effort to have the telecommunications industry offer a secured version of their products. Where there is direct and obvious benefit to the government and to the vendor, NSA will supply to qualified vendors cryptographic techniques and standards (under strict control agreements) for the purpose of integrating a COMSEC function, at vendor expense, into his product. If done in accordance with its standards, NSA will endorse it for use. The vendor is then free to market his secured product to authorized users. Different cryptographic techniques and standards will be available for different markets (e.g. products targeted for the classified information market and products targeted for the sensitive information market). Sales will, in general, be restricted to U.S. owned and controlled entities.

Currently there are a number of vendors involved in both of these programs. The CCEP in particular will be quite an extensive effort and holds the most promise for bringing widespread COMSEC availability.

V. National COMSEC Assessment Center (NCAC)

Since National Security Decision Directive 145 was signed in September last year, many efforts have been underway to realize its direction. One of these is in response to the requirement that the NTISSC submit an ANNUAL EVALUATION of the status of National Telecommunications and Automated Information systems Security to the Systems Security Steering Group. This will replace the Biennial Report which was last submitted in February 1984.

The National Manager has established a National COMSEC Assessment Center in the Communications Security Organization at NSA to provide a continuing program of assessment of the nation's communications security posture. This center has already begun to work with the departments and agencies of the Government and its contractors to ensure that SENSITIVE communications are identified and provided appropriate protection. The results of this collaborative effort will constitute the NATIONAL COMSEC

ASSESSMENT PROGRAM, and will provide a firm foundation of documented vulnerabilities upon which to base requirements for COMSEC resources and to prioritize programs for national COMSEC planning and management. The assessment will include the vulnerability and threat to electronic word processing systems, as well. The first data call has gone out to all department and agencies of the government. Response to this data call is due 1 October 1985. Upon receipt of the data call information, the NCAC will prepare its first "Annual COMSEC Assessment Report" for publication by 15 January 1986. Although this will be the National Manager's assessment, it doubtless will be used by the NTISSC subcommittees as the basis for their annual evaluation as well.

VI. Legislative Initiatives

In the area of foreign cryptography control, foreign enterprises are manufacturing cryptographic equipment and can be expected to try to market it to the United States Government and its contractors. The equipment could be subject to hostile exploitation and manipulation during both the manufacturing and shipping phases. Legislation is required giving NSA the authority to regulate the purchase or use of foreign-manufactured cryptography by the United States Government and its contractors. This security driven necessity of regulating the suppliers of COMSEC systems to essentially U.S. firms has a significant added advantage to U.S. industry in terms of foreign competition.

In order to provide a distinct incentive for U.S. industry to purchase and use COMSEC equipment for its business telecommunications and information systems and at the same time protect against well-documented hostile foreign exploitation of a vulnerable and lucrative target, we suggest that an amendment to the Internal Revenue Code to provide tax credits to U.S. businesses which purchase such equipment be explored. The present tax code provides for deductions for capital equipment, amortization, and investment tax credits. This legislation would encourage the purchase of communications security protection by allowing a tax credit. This legislation would encourage U.S. business to purchase communications security equipment that will protect advanced technological information, company proprietary information, and other sensitive information in the National interest. It also will encourage U.S. companies to develop communications security equipment to protect the new communications products that are being sold to industry.

VII. Closing

Mr. Chairman, this document has discussed at length the organization and the structure of our national telecommunications and information systems structure in the wake of NSDD 145. We have shared with you and the members of this subcommittee one perception of some of its accomplishments, and of some work that needs yet to be done. We have suggested legislation in the areas of a Consolidated National Telecommunications Security Program, controlling the use of foreign cryptographic equipment, and tax incentives for private sector COMSEC.

STATEMENT OF

ROBERT L. BROTZMAN
DIRECTOR, DEPARTMENT OF DEFENSE COMPUTER SECURITY CENTER

AT HEARINGS
BEFORE THE

SUBCOMMITTEE ON TRANSPORTATION, AVIATION
AND MATERIALS

COMMITTEE ON SCIENCE AND TECHNOLOGY

U.S. HOUSE OF REPRESENTATIVES

JUNE 1985

Good morning Mr. Chairman. My name is Robert Brotzman and I serve as the Director of the Department of Defense Computer Security Center, and also as the Chairman of the Subcommittee on Automated Information Systems Security of the National Telecommunications and Information Systems Security Committee. Thank you for this opportunity to describe some of the activities of the Center, and of the Subcommittee, which support National Security Decision Directive Number One Hundred and Forty-Five.

The computer is today's prime force for change. It is reshaping our lives in the second half of the century, just as the automobile and plane did in the first half, and industrialization did in the second half of the nineteenth century. Every blessing, however bountiful, carries with it its own curse. Invariably, our initial enthrallment with the beauty blinds us to the blemishes. We have difficulty bringing ourselves to deal with the problems until well after we have become addicted to the pleasure. For many decades, we accepted the convenience of the automobile as an unmixed joy. Then one day we awoke to find a polluted atmosphere, fifty thousand auto-related deaths per year, a public transportation system in shambles, and a dependence on foreign oil that imperilled our economy and our security. We are now confronting those problems, at great cost and with limited success. None of these problems arose overnight; and each could have been dealt with more easily, cheaply, and successfully had we the foresight to recognize and the will to solve them earlier.

The clock moves only forward. We cannot turn away from this new revolution, the computer revolution, nor would we want to do so. It serves us well. The computer is assuming our burdens on tasks that are tedious, and giving us the power to break through barriers that once seemed insurmountable. In alliance with other technology, it is expanding the forms, speed, reliability, and extent of our communication systems.

To enable this immensely talented servant to do its job, we have entrusted it with our knowledge base. The computer has become the custodian of our defense secrets, financial accounts, scientific data, proprietary information and personal records. Nearly all information that matters that is not already recorded in some computer soon will be. We have expended enormous resources to teach the computer to manipulate, to retrieve and, more recently, to make inferences about the information it generates or is fed. Our success has been monumental and a momentum has been built which ensures that future success will be more rapid and more profound. But our success, like our effort, has been largely limited to increasing the utility of the computer. We have taught it much about how to use its knowledge base, but little about how to protect that knowledge base from improper use.

In recent years we have learned of incidents of misuse of credit files, unauthorized access to medical records, disruption of public services, and some fairly large embezzlements of funds through malicious use of computers. These incidents would be judged as trivial if compared to the havoc which could happen if a desire to cause great harm becomes united with the technical skill to do so. This union can happen at any time. It is especially likely to happen because of electronic bulletin boards. People who are probably motivated by technical curiosity, discover weakness in computer systems (and there are many there to discover) and explain those weaknesses, and how to exploit them, on electronic bulletin boards. There, anyone, independent of technical sophistication may read of these techniques and learn how to use them. I am sure that the ability to cause great harm with very little effort or expense is appealing not only to our traditional enemies, but to terrorists, or to people with a grudge against society. Such destructive acts are even more attractive when they can be carried out anonymously.

The greatest single danger to computer security today is the utility with which today's vendors and buyers seem most enamored -easy access. While the proliferation of personal computers has vastly enlarged the user population, modern networking has permitted those computers increased access to automated data bases throughout the world. The utility of having massive arrays of information quickly and easily available to a broad spectrum of people is obvious and attractive. But this capability can be used constructively or destructively. It can enable both the honest worker and the scoundrel to do his job more effectively. Opportunities - whether for good or for evil - draw like a vacuum. Where they exist, they will be seized. Retaining the usefulness of nearly universal logical access while guarding against its dangers will be an awesome technical challenge. It will amplify both the need for security features, and the difficulty of designing them.

The jeopardy that insecure computer systems imposes to our security, our economy and our personal freedom will increase in proportion to our dependence on those systems. That dependence is accelerating. Federal programs ranging from national defense, intelligence, space, air traffic control, health, social welfare, and financial activities rely on computer support. Computers are essential components in our weapons systems. Most major governmental activities could not meet their mission objectives without the use of computers. Many of the critical activities within the private sector have a similar dependence on computers.

The computer industry of the United States is a hundred and forty-billion-dollar-a-year Juggernaut, growing at a rate of sixteen to twenty percent per annum, and proceeding relentlessly down a risky road. We seek to divert that rambling giant on to a different path; a path that includes good security features right along with high utility. In order to succeed, we need to obtain extraordinary leverage from every dollar, because the industry to be altered dwarfs the resources we have committed to effect that alteration. We are in a race in which holding our own now would be a remarkable achievement, but failure to close the gap cannot remain an acceptable option.

The inherent ability of current computer systems to protect themselves and their data from abuse is appallingly low. Treatment is available right now which can improve their ability to function securely, but nursing systems that were born weak is only a stop-gap, not a solution. To reduce our risks substantially, we need to develop and apply methodology that will enable us to create systems with solid security features designed in from the beginning. To build these robust systems and ensure that they retain their strength requires not only excellent design, but also excellent maintenance procedures, to prevent accidental or malicious damage to the security mechanisms. Research is needed to figure out better ways to implement security technology which we now understand; research is also needed to figure out how to design and build machines which have security properties far superior to anything now in existence.

The strategy we are pursuing consists of a three-pronged attack; firstly, we are encouraging the use of software packages which can reduce the risk to many current systems. Our goal is to have password protection systems and audit controls in use on all governmental systems which need such protection within two years. Secondly, we are encouraging industry to develop systems defined in the Department of Defense Trusted Computer Systems Evaluation Criteria. Our goal here is to have computer systems which will support a stringent access control program in use on government systems which need that level of protection before the end of the decade. Thirdly, we are embarking upon an aggressive research program to substantially improve the state of knowledge about computer security. In general, this strategy attempts to do immediately those things which we know how to do, and to proceed in parallel to try to improve the medium - term security posture and start the research program needed to learn far more about the subject.

The effect of any research activity we initiate today will not be felt in practice for over ten years. The time from conception of an idea until we can obtain budget money to pursue that idea takes about two and a half years. There is a time lag between the time one starts applying resources to a problem, and the time that some useful results are available. The gestation period for industry to develop a computer security product is about five years. At least another two years will pass between the time a product enters the market and the time it begins to have a substantial impact on operational systems. We have already missed our opportunity to influence the fifth generation computers and the personal computer explosion. We can influence the technology of the middle nineteen nineties only if we move aggressively right now.

The demand for secure computer products and their availability will drive each other. Not many people voice needs which they believe cannot be satisfied. A lack of available secure products can mute even buyers who are aware of the threat imposed by insecure systems. The vendors, interpreting the quiet as a lack of interest, will be slow to develop for a market which they see to be small. If we can increase users' awareness of their vulnerability, and of what can be done right now to reduce it, we will expand the market, and vendors will be encouraged to develop products for it. If we can encourage vendors to develop more and better secure products, we will activate the latent market that now perceives a need but no remedy.

Protecting information and ensuring that computing services will not be denied are concerns of both the governmental and private sectors. Capabilities that help one sector will be applicable in the other. Even a well-focused campaign to obtain secure systems for the government will yield progress that is too little and too late without the partnership of the private sector. The government's five percent share is inadequate to drive the market. We must convince the private users that they cannot remain passive in the endeavor, but must actively demand and employ good computer security products.

To support a future structure of secure systems, we will need to lay a strong and enduring foundation. The key part of that foundation must be standards that are appropriate, well-defined, and widely accepted. Since quality tools are of little value when placed in inept hands, we must develop guidelines for employing computer security tools. Training, appropriate to the roles of administrators, computer operations personnel, and general users, will need to be provided.

We at the Computer Security Center believe we can best achieve our objectives by adopting a philosophy of openness to the needs of the agencies we serve and to the ideas and participation of all who can contribute. Computer security cannot be established by decree or created by the work of any single organization. If we are to have wide-spread availability of trusted systems, it must be through the cooperative efforts of government, industry and academia.

In the nine months since National Security Decision Directive number one-forty-five was signed, a number of initiatives - both within the structure of the National Telecommunications and Information Systems Security Committee and within the Computer Security Center -have been undertaken toward implementing the structure, fulfilling the objectives, and carrying out the policies of that document.

The Subcommittee on Automated Information Systems Security has conducted five formal meetings, and the four working groups of that subcommittee have already met a total of twenty-one times.

Working Group Number One was formed to perform the annual evaluation of the status of automated information systems security. It is chaired by Mr. Edwin R. Lindauer, Jr. of the National Security Agency. The group generated the report in February and then proceeded to begin work on next year's report. They have determined a schedule of activities which will lead to the delivery of a report to the full Subcommittee in January of 1986.

Working Group Number Two was formed to help with the computer security assessment questionnaire which the Office of Management and Budget distributed early this year. It was chaired by Mr. F. Lynn McNulty of the Department of State. It has completed its task and has been disbanded.

Working Group Number Three was formed to generate definitions, standards, and criteria. It is chaired by Mr. James Burrows of the National Bureau of Standards. This working group has maintained close coordination with a parallel group established by the Subcommittee on Telecommunications Systems which is also working on definitions of "sensitive" data.

Working Group Number Four was formed to draft policy on automated information systems security. It is chaired by Dr. Neil Stillman of the General Services Administration.

The subcommittee has submitted its first annual evaluation report on the status of the security of the nation's automated information systems. That report was sent to the parent committee in February of this year. To support the subcommittee, a full-time Secretariat has been established. This Secretariat carries out the coordination needed to sustain subcommittee activities.

Within the Computer Security Center, the changes that National Security Decision Directive One Forty-Five has brought to our mission are reflected in the draft of our new Charter, which is now being coordinated, and in our activities. Before I relate how we have redirected the emphasis of our activities, I would like to outline a few of the assumptions we made about the nature of our new mission and the conditions under which it would be performed.

National Security Decision Directive Number One Forty-Five not only expanded the scope of our mission, it changed the nature of our clientele. Most civil agencies are less aware of their computer security needs than are the agencies and departments of the Department of Defense. To the extent that they do recognize those needs, they apparently perceive them as quite different from those within Defense. To service this new community, we will have to raise their awareness, gain an understanding of their computer security concerns, and determine which of their needs truly are unique and which have common threads. We do not have all the answers for the problems of the civil sector of government; and if we did, those answers could be applied effectively only if the people concerned recognized them as valid. There will be no salvation in a forced conversion.

To raise awareness of the computer security problem, we have provided speakers to numerous conferences and courses. Two computer security awareness films produced by the Center will soon be ready for national release. Within three days of announcing the availability of the films in Government Computer News, we were contacted by more than one hundred agencies and organizations seeking copies of them. Over the next few years, we expect to produce several films and video tapes on subjects such as password management and the Trusted Computer System Evaluation Criteria.

The initial steps have been taken towards developing and implementing an education and awareness program. Through this program, we expect to train or influence a massive audience, primarily, but not exclusively, within the government, to be aware of the need for computer security and of the techniques for maintaining it. Security literature and posters will be distributed, "awareness exhibits" will be provided at symposiums, and a variety of awareness training will be given. A National Training Plan has been drafted to address computer security on a national, vice Department of Defense, level. Some existing computer security courses are being modified to remove classified material so that they may be given to a wider audience. The annual conference, which is sponsored jointly by the National Bureau of Standards and the Computer Security Center, is being refocused to better include the civil government and private sector audiences.

To gain a better understanding of our new clientele, we are initiating an education needs assessment program for the federal government. To extend our knowledge of security problems beyond government circles, an effort has begun to study computer abuse in the private sector. We have established informal contacts with agencies such as the Department of Energy, the Department of Commerce, the Federal Bureau of Investigation and the General Services Administration. A survey of Defense Department contractors' use of hardware and software, similar to that done for the Department of Defense, is now underway. We have responded positively to requests for assistance from the Federal Emergency Management Agency, the Forestry Service, and the Treasury. In providing these agencies with the assistance they requested, we are gaining a greater understanding of their needs.

An introductory letter has been prepared to explain the Center's services to our customers in the civil government departments, and to ask them to designate an initial point of contact. We see this as a step towards establishing a network of computer security experts to orchestrate internal programs and to serve as a communication channel between their Agencies and the Computer Security Center.

The Center has begun to analyze the security implications of personal computers and office automation, and of the local area networking that will expand their utility. Our purpose in conducting these studies is to gain understanding of the procedures which can be used to reduce the risks inherent in using current hardware and software products. The results will be widely distributed in the form of guidelines and standards.

Within the jungles of hardware and software that comprise computing systems lurk predators - those that can savage suddenly, leaving obvious wounds, and those that can bore silently, slowly infecting a system. Knowing the nature of the danger and where it lies concealed can enable us to avoid it. To gather this knowledge, we have developed a Computer Security Vulnerability Reporting Program. This program is now ready to be submitted to the Assistant Secretary of Defense for Command, Control, Communications and Intelligence. It will require reporting of any computer security vulnerabilities discovered within Department of Defense systems. The purpose of the program is to increase our knowledge of the state of security within Defense systems and, as appropriate, to initiate remedial actions to correct reported vulnerabilities. Once the program is established within the Department of Defense, we intend to invite the rest of government to participate.

We plan to use talent that lies outside the Center to do much of the work of evaluating systems and products. A program is being developed to train evaluators, both those within the Center and those in other agencies. We have undertaken an aggressive hiring program. While there are few people with computer security experience available for hire, we are succeeding in recruiting people with strong academic backgrounds in computer science, engineering, and the other basic disciplines which we require. In the long term, our new hires show promise to become important assets to the Center. In the short term we will be drained of some of the talents of our more experienced people whose time must be diverted to turning our new people into adroit computer security specialists.

Through our awareness program and our efforts to acquaint both the governmental and private sectors with the threat imposed by insecure systems, we hope to engender an uneasiness about the status quo that will spark demand for additional computer security products. We are establishing contacts with computer user groups in order to encourage them to voice their concerns about inadequate computer security in the development of new products and services. We are also developing guidelines which, at least within the Department of Defense, will make it easier to determine and specify the level of security that a system needs when generating requests for procurements.

Within the Center, we plan to build an automated data processing operation that can serve as a showcase for the departments and agencies of government so that they can see how security features can be applied in today's operations.

A new division has been created to interact with the commercial world and to encourage vendors to consider security in the design phase of all their products. In March of this year, we sponsored a conference for computer vendors which was attended by about two hundred people from industry. We intend to make this an annual event. We have met several times with the Computer Business Equipment Manufacturer's Association and a promising relationship is being developed with that body.

While to date it has only been published as a Computer Security Center document, the Trusted Computer Evaluation Criteria (commonly known as the "Orange Book") is widely accepted as the authoritative document in that area. About twenty-two thousand copies have already been distributed. Coordination is nearly completed now to make it a Department of Defense Standard. Now that our mission has been extended, efforts are underway to determine the revisions needed to make the "Orange Book" more applicable to the civil sector.

An "environmental guideline" document that provides guidance on how to use the "Orange Book" is about to be published as a Computer Security Center document. It too will be revised as necessary to meet the needs of those outside the Defense Department. We expect to produce a guideline document on Magnetic Remanence within a few weeks. A guideline on Password Management is being published by the Center and we expect to present it as an appendix to the National Bureau of Standards Password Standard to the National Committee at its August meeting. We also have begun to develop Audit Guidelines, Discretionary Access Control Guidelines, Network Security Criteria, Data Base Management Criteria, and Office Automation Security Guidelines.

We have accomplishments of which we are proud and have made a good beginning on a number of initiatives that we expect to be productive. But we have not done -- or even started - everything that it would be useful to do. Our resources - especially in terms of skilled technical people - won't stretch that far. For example, we have already had requests for evaluations by 14 civilian agencies. Each of these requests represented a need. To date, we have only been able to undertake two such projects.

The threat imposed by insecure systems is one that has to be addressed. It isn't just a Department of Defense problem, although the threat to our security is paramount. It isn't just a governmental problem. It looks over virtually every aspect of our lives, collectively and individually - public and private. There are no panaceas, but there are steps that can be taken to reduce the danger.

We need to take these steps as quickly as our capabilities allow. Whatever can be done now, should be done now. Whatever is postponed will be harder to do and probably more expensive in the future, but what's worse, postponement means a longer time of having to depend upon systems that are all too vulnerable.

The structure created by the National Security Decision Directive One-Forty-Five has raised the level and broadened the scope of attention given to computer security. This was an important prerequisite for dealing successfully with this universal problem. Within the Computer Security Center we have charted a course which we believe to be responsive to the task set before us. We are aggressively pursuing initiatives that address both current and future needs. The actions we are taking come with no guarantees; failure to act does carry a guarantee - that of a major disaster.

I am grateful that the committee also views these problems as serious and is taking the time to examine them. With your support, we believe our chances of staving off a disaster are greatly improved. There will be enormous difficulty in providing adequate protection to the nation's information base and the equipment which processes that information. If we do it and do it well, we will survive as an information-based open society! That is well worth doing.

Mr. **Glickman.** Our next witness is our colleague from the State of Texas, the chairman of the House Committee on Government Operations, Mr. Jack Brooks.

Mr. Brooks, it is a delight, and I underline that word, to have you before this committee, and I know that you are a man of—I was going to say of very few opinions, but I would say that would be an understatement, to be sure—and I know you are interested in this subject matter very much.

We are delighted to have you here.

Mr. **Nelson.** Mr. Chairman, could I interject a statement there?

Mr. **Glickman.** You may, yes.

Mr. **Nelson.** I just want to say that Mr. Brooks has been absolutely delightful to work with, since the Johnson Space Center is in his constituency, and we have protected it from being closed down, and moved elsewhere, and I will continue to protect his interests.

Mr. **Glickman.** I am sure that Mr. Brooks is most appreciative of the fact that you are here today and telling him that.

STATEMENT OF HON. JACK BROOKS, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF TEXAS

Mr. **Brooks.** I am that, and I am very pleased to appear before your committee, Mr. Chairman, and to receive the warm welcome from you and the very distinguished Member from Florida, Mr. Nelson.

I want to say that I am very pleased to be a coauthor with you, of your bill, to protect Government computers from outside threats.

I have been aware of that need and that problem for probably 20 years. The Government has done very little about it, a problem that has always been there.

If one of these eggheads can design a computer in an ivory tower, he can design a way to get into it. And anything that has been built is old and passé. Because the new ones are still on the drawing board, and the real good ones are still in some physicist-mathematician's mind somewhere being dreamed up. They haven't even put it on paper yet, but that will be the one that is the next one.

So the leading edge is still way out there, and if you think those people can't break into the existing hardware, you are crazy. They can, and they do. And the Government has done very little about it.

Private industry has also done very little. It is the horror story they don't like to talk about. It scares them to death. All their records could be destroyed in private business. It is very dangerous, and they have done very little about it.

They keep trying to make some peripheral efforts, but they have been very lax about it, private industry and the Government, and every effort to get the National Bureau of Standards to continue to study, and to make those kind of changes, has been fought by this administration, which continues to cut their appropriations every year.

Well, so much for that. We will work on that this afternoon. But, Mr. Chairman, and members of the subcommittee, I want to say I appreciate the opportunity to provide my comments on the National Security Decision Directive, NSDD 145, "Big Brother Is Here. 1984 Is With Us Now! Have You Taken Your Polygraph Today?"

It is going to be like a blood test, you take the polygraph every day. When you kiss your wife goodbye and say, "I love you, darling," do you take a polygraph right then?

It is my understanding, and I hope the House could buy a polygraph that would be available to the wives of Members of this Congress and the committee staff, that they would be able to bring him down by the ear and hook him up, and ask him a few of those questions.

"Where were you?" I think it would be fascinating. And if it works, those wives would already have one. And if it works, why don't they give them to those idiot contracting officers who steal all that money, who have all those cost overruns. Don't worry about spies, worry about those people that are wasting billions of dollars, because they don't write good contracts and there is a "little" overrun and there is a "little" overcharge. We should ask those contracting officers.

And why not ask the contractors, too? Let everybody at General Dynamics, and all the space operations, take the polygraph tests when they sign a contract. "Did you lie about this bill? Did you lie about the charges? Are you double-dipping?" I think it would be fascinating.

At any rate, the national policy on telecommunications and automated information systems security, that "great" directive, I want to commend you for your efforts to review it.

It is important that the Congress and the American people fully understand this directive, its purpose, and the effect that its implementation would have on our Government and its citizens.

According to the administration, the purpose of the directive is to counter the growing threat of foreign exploitation of computer-based information systems within both the Government and the private sector.

Admittedly, this is a laudable goal. However, I believe that NSDD 145 is one of the most ill-advised, potentially troublesome directives ever issued by a President, and they have issued a good many, you know. That is a pretty high honor, to be one of the worst.

It seeks to vest in the Department of Defense, that "paragon of virtue," that "polygraph heaven," the authority—they are all going to be honest out there, because we have got the polygraph—4 million people going to be taking them as of last night if the conferees don't have enough sense to knock that hocum out of the bill—this directive seeks to vest in the Department of Defense the authority to establish regulations and standards which would govern the access to and the processing of all computerized information which it deems—which it, on its own volition—deems to be critical to the national security of the United States.

Now, that might be the price of butter. It can be anything they want it to be. This would include not only classified information, but any other information within the civilian agencies, which the Department considers sensitive.

"Where were you last night? It is sensitive."

The directive would also give the Department of Defense the power to influence the collection, the processing, the dissemination of information in the private sector, whenever it believes it would be in the interest of national security.

Are they going to lock up all the AP wires? Are they going to double-check all the sensitive information that the media utilize from time to time when they make comments or analogies or conclusions on the radio, on television, in the hard press?

Since it leaves it up to the Department to define what is in the interest of national security, virtually any information, the information system located in the civilian agencies or in the private sector would fall under its domain.

Now, they are not going to tell you that they are going to do that now. But it is in this kind of a directive that they would have that authority. It means that Big Brother is really here, and all they have to do is implement this to control the press, to control private business, and one set of people out there is setting that standard.

Now, maybe that is the new American way, the new hysteria of 1985, but it isn't like the American way with which we were raised.

In my view, this directive is seriously defective on several grounds. First, it was drafted in a manner which usurps Congress' role in setting national policy. Under our system of Government—I mean in the past, the system we have lived under all these years—the Congress, under the Constitution, had the sole responsibility for setting national policy through the enactment of legislation.

And the President has the duty to faithfully execute the public law. I realize that that is old-fashioned under the Constitution, and it has just been with us a couple of hundred years, but it doesn't really work any more, according to them.

But under this operation, while the President has proclaimed that NSDD 145 sets national policy for telecommunications and computer systems security, he has no real legal authority to do so.

This is not an esoteric issue. The corridors of the Pentagon, the offices of the east wing of the White House, whether it is under Democrats or Republicans, are not places where national policy should be established.

The importance of this issue demands public hearings and a full debate in Congress before the national policy is set, but I would like to hold up on that debate for just a week or two, until they get over the latest hysteria, if they can.

After last night's performance, you can understand that this is a very nervous Congress.

Second, the directive is in conflict with existing statutes, which have assigned to the Office of Management and Budget, the Department of Commerce and the GSA the sole responsibility for establishing government-wide standards, guidelines and policies for computer and telecommunications security.

In the existing NSDD 145, the President ignored the statutory authorities and unilaterally transferred these responsibilities to the DOD. Once again, the President does not have the authority under our constitutional form of Government to unilaterally revise existing statutes.

If the President believes that the DOD could do a better job, then he should have proposed legislation to the Congress to legally effect this change.

Finally, I seriously question the wisdom of the President's decision to give DOD the power to classify, and hence, to control information located in all the civilian agencies and even the private sector, which in DOD's opinion may affect national security.

One of the benefits of a full and open society is the rich exchange of ideas and knowledge, unfettered by government intervention and red tape. The successes of our scientific, technical and medical communities have been based upon the free exchange of data and information.

And since it is a natural tendency, understandable of DOD, to classify everything, it would be impossible for the Department to strike an objective balance between the need to safeguard information and the need to maintain the free exchange of information.

They could not help but have a propensity and a tendency to classify almost everything, because everything has some influence on the Government, on the economy, on our security, almost everything.

There are other practical problems as well. DOD does not have the resources to classify and control all the information that would be encompassed by this directive. And furthermore, the cost of applying DOD security-type measures to civilian agencies and private sector information systems would be overwhelming. Where is all that money going to come from?

In my opinion, DOD has its hands full, trying to even modestly protect its own classified information, and I think it would be foolhardy to expand its jurisdiction to protect the unclassified information contained in civilian agencies and in the private sector.

In summary, NSDD 145 is seriously flawed in both legal and practical terms, and ought to be withdrawn. This does not mean that there is not an urgent need for greater attention to be placed on the protection of unclassified but sensitive information.

There is no question that the civilian agencies have fallen behind in implementing computer security measures. However, this has been caused primarily by a lack of attention to this area and by inadequate funding.

They just haven't focused on it. Current technology offers the Government and the private sector a multitude of means to protect its sensitive areas for a price. Agency heads must be made aware that more resources must be allocated for computer and telecommunications security, including proper training for agency personnel in this area.

The National Bureau of Standards is in the best position to assist the agencies in this effort, and I would urge the subcommittee to consider this alternative.

Thank you very much.

Mr. GLICKMAN. Thank you, Mr. Brooks, for an excellent statement.

Let me just ask you two quick questions. I gather from your statement that you believe that there are statutory and maybe even constitutional problems with the delegation of this kind of authority to the Department of Defense and the National Security

Agency to basically manage computer security and telecommunications security in the private and civilian sector.

Is that a fair statement?

Mr. **Brooks**. It sure is a very fair statement, an accurate statement, I might add.

Mr. **Glickman**. And the other thing is——

Mr. **Brooks**. We have existing laws, you know, that assign to the Office of Management and Budget, the OMB, the Department of Commerce, and the GSA, the sole responsibility under the law—we have signed that—the President signed it, Congress has passed it.[2] Oh, that doesn't mean that it is a law, but I mean it happened that way.

And those agencies have been given the sole responsibility for establishing Governmentwide standards and they have done a pretty good job on that. It has been slow, they should work at it a little more, setting guidelines and policies for computer and telecommunications security. But they are the people that should be considering security, not a new group.

Mr. **Glickman**. Well, you know, I am sure this thing did not—this directive did not go through the Federal Register, and did not go through the normal regulatory process. And I am also reasonably confident that it did not go through the standard OMB review that OMB likes to have with respect to agency regulation.

I guess one of the things that concerns me is that you have granted a whole new way to provide computer security in this Government without public input into that process.

Mr. **Brooks**. That is correct.

Mr. **Glickman**. I mean, you might have had some——

Mr. **Brooks**. Or without congressional input. They just decided what our new policy is going to be. Congress has not passed this. The President hasn't signed it. They just issued a unilateral decision of how they are going to run it.

Mr. **Glickman**. Yes, I mean in substance, I have some concerns, but the process is something that does concern me, and I think that is something that folks who are involved in this ought to again look at, because you know, I think that there might have been some input from agencies, but it was done on an informal basis.

Mr. **Brooks**. Do you know which agencies?

Mr. **Glickman**. No; we can find out, but I mean in terms of civilian agencies——

Mr. **Brooks**. You can almost guess.

Mr. **Glickman**. Well, the discussion and the testimony was that some civilian agency like Treasury was involved in this, and that may be fine, but again, I doubt that there was any public input into this process, at least in any formalized type of way, and that again is what we tried to protect the public, when we designed administrative procedures acts in those kinds of things.

Let me also ask you, I asked the question, isn't it clear that, let's say, the military is in charge of this effort, and the answer was, well, the NSA is not a military agency. It is a service organization that provides services to the intelligence community, but now provides services to civilian agencies as well, in terms of computer security.

---

[2] This sentence should read, "We have existing laws * * * sole responsibility under the law Congress passed."

I wonder how you would respond to the allegation that the NSA is a military agency, and therefore——

Mr. **Brooks**. They don't call it the GSA—the National Security Agency has normally been closely aligned with the Defense Department in security efforts, and I am sure that it still is, and it doesn't make a cottonpicking bit of difference what they say, that is what they do.

Now, they would be willing, I am sure to assume responsibility for every department in the U.S. Government, and every industry within the United States, all the private sector, they would be willing to run it all, but God knows what a shambles it would be if we turned private industry over to the NSA or to the Defense Department. It just isn't good business.

I don't believe they are smart enough to run the whole country, and neither do the people that manage those industries, and if they suck into this deal, they will be taking orders from somebody declaring what is sensitive information for every major industry in the United States, steel, chemicals, oil, banks, financial institutions, agricultural co-ops, they can run it all. It is all important, to some extent.

You want those people running our industry? I think it would be a disaster.

Mr. **Glickman**. You talked a little bit about the National Bureau of Standards. Do you think that—and you acknowledge in your statement that the civilian agencies haven't done a very good job in computer security.

Mr. **Brooks**. That is correct.

Mr. **Glickman**. Do you think that the NBS can be beefed up to provide some of the necessary help to civilian agencies——

Mr. **Brooks**. Of course, they have been fighting for their appropriations. You have got to give them enough money to do some work on security measures and countermeasures. This is highly possible, the state of the art in that field is fairly well advanced, there are a lot of things they can do.

For example, quit taping your password to your desk, in case you forget it, so everybody in the building knows what it is, and eight people that clean up. You know, just ordinary, reasonable precautions are not even utilized in many instances, and anybody can go into the computer room.

There are very few controls, and there are many new systems to limit access—handprints, voiceprints, fingerprints, footprints—everything under the Sun. And then we always have the polygraph to rely on. That will be a big help.

Mr. **Glickman**. Well, Mr. Brooks, we are most appreciative that you came down here today.

Mr. **Brooks**. It is a pleasure to be with you.

Mr. **Glickman**. Thank you very much, sir.

Our next witness is Mr. Warren G. Reed, Director, Information Management and Technology Division at the GAO.

Mr. Reed, I don't know, that is a tough act to follow, but we don't require the same level of humor of every witness, I can assure you of that.

STATEMENT OF WARREN G. REED, DIRECTOR, INFORMATION MANAGEMENT AND TECHNOLOGY DIVISION, U.S. GENERAL ACCOUNTING OFFICE, WASHINGTON, DC, ACCOMPANIED BY WILLIAM FRANKLIN, ASSOCIATE DIRECTOR; HAROLD PODELL, GROUP DIRECTOR, INFORMATION MANAGEMENT AND TECHNOLOGY DIVISION; AND RAYMOND WYRSCH, SENIOR ATTORNEY, OFFICE OF GENERAL COUNSEL

Mr. Reed. I am glad you said it, thank you.

Mr. Glickman. You may proceed any way you deem appropriate, and your entire statement will appear in the record, so if you want to summarize or whatever you have is fine with us.

Mr. Reed. Thank you, Mr. Chairman. I will summarize my statement.

I am pleased to be here today to contribute to the examination of this directive that we have discussed quite extensively so far.

You may recall that I testified before your subcommittee back in 1983. At that time——

Mr. Glickman. Same subject, I think.

Mr. Reed [continuing]. Identified a number of problems on the same subject. What I would like to do is——

Mr. Glickman. Why don't you introduce the folks with you, too.

Mr. Reed. Yes; I have with me Mr. Bill Franklin on my far right; Ray Wyrsch from our Office of General Counsel; and Dr. Harold Podell, up there, who is going to display in a moment a prop I am going to use, just briefly.

What I would like to do is just take a moment, perhaps, to use a chart I have to characterize some of the things I have—that we have been talking about, and in particular, the environment that existed before you issued your report, your committee report from your last hearings.

OK, Harold.

What you really see characterized in this chart [fig. 1] is quite simple, I think, in terms of the message and bottom line, and it really relates very directly to what Congressman Brooks was just talking about, where we are trying to characterize the environment as it existed before the directive that we have been talking about arrived on the scene.

OVERVIEW OF CRITICAL NATIONAL SYSTEMS

Policy/Standards Guidance	OMB; GSA; Commerce; OPM		
Line Management	EXECUTIVE AGENCIES		
S Y S T E M S	National Command and Control Systems Tactical Command and Control Systems Defense Intelligence Systems . . .	Defense Financial Management Systems Defense Inventory/ Supply Systems Federal Reserve Wire Transfer System National Crime Information Center FAA Air Traffic Control System Power/Water Control System Hazardous Materials Tracking System . . .	IRS Systems Social Security Systems DOD, VA Patient Care Systems Crop Forecasting Systems Federal Reserve State Bank Supervision System Treasury Financial Communication System Treasury Bill Book Entry System . . .

FIG. 1

We have the central agencies shown that Congressman Brooks talked about, who have had essentially the overall national policy standards and guidance to executive agencies' responsibility, established by existing statutes.

We have had the line management by the executive agencies themselves. And the thing I wanted to really focus on in this chart, Mr. Chairman, are some of the systems that we have been talking about, particularly the context in which they were viewed before the directive 145 arrived on the scene.

What you see to the left of the—the systems you see to the left of that dashed line that is running vertically are the more traditional defense and intelligence systems characterized in generic form, national command and control, intelligence, and so forth.

And what you see on the right of that dashed line are some of the systems that have been referred to this morning as sensitive, unclassified, some of which are in the defense community themselves.

But in the middle column, you will see the kinds of systems that perhaps may have some kind of national security bearing, and you will see on the right, some systems that are a big question mark in terms of the IRS systems, Social Security systems, some of the——

Mr. **Glickman**. Why not, for the record, we read—you are listing in the left column, systems, if I read them—defense financial management systems——

Mr. **Reed**. Yes, that is correct.

Mr. **Glickman**. Defense inventory supply systems——

Mr. **Reed**. Yes.

Mr. **Glickman** [continuing]. Federal Reserve wire transfer systems——

Mr. **Reed**. Yes.

Mr. **Glickman** [continuing]. National Crime Information Center, FAA Air Traffic Control Systems, power water control systems, and hazardous materials tracking systems.

Mr. **Reed**. Yes.

Mr. **Glickman**. Now, you have basically defined those as systems that could be classified as sensitive systems?

Mr. **Reed**. They could be. My main point is there is a large collection of systems previously unclassified and associated with the civilian community.

My main point is that those systems to the right, which include those you just read from the chart, of that dashed line, are systems that traditionally have been considered part of the civilian community within Government. They have been largely, mostly unclassified, and I will come back to that chart later, and perhaps address the clarification I think that you are——

Mr. **Glickman**. But the other systems on the far right, the ones I did not read, systems like IRS, Social Security, DOD VA patient care systems, crop reporting with the Department of Agriculture, Federal Reserve, State bank supervision systems, Treasury financial communications systems, Treasury bill book entry systems.

Are those classified different than the first group of systems I read? Or are they in the same category?

Mr. **Reed**. The only qualification I would make of those systems is that it might be more difficult to establish a correlation with national security of those systems, as contrasted, say, to the systems listed in the middle column or the column on the left.

Mr. **Glickman**. I understand.

Mr. **Reed**. All right.

Anyway, I thought that might be useful in helping the perspective of the discussion that we have had so far, and the rest of my discussion.

I would like to just emphasize that I believe your 1984 committee report reinforced the critical nature of the increasing vulnerability of the systems that are indicated up here, and it further emphasized that those systems operating under the civilian elements of Government were especially vulnerable and required special attention.

I might also add that we will be reporting to you, I believe, in this fall—the fall time frame, where we are examining 18 of the line agencies referred to up there, and specifically, sort of the status vis-a-vis the health of their security problems of at least 25 major systems of the sort that I have indicated up here on that chart.

I would like to just characterize the recommendations of your 1984 report again, because they are important to us in our examination of the directive that is being examined today.

We understood your recommendations to the administration, generally calling for an immediate assessment and analysis of the problems and issues associated with the critical national systems, and particularly the civil systems.

And you additionally called for a strengthening of the organizational arrangements, so that national policies could be developed and implemented to ensure appropriate safeguards for critical national systems.

As we have discussed this morning, the two main initiatives that have developed since your 1984 committee report, have of course been the directive and the draft circular from OMB, and I would like to just focus the rest or the remainder of my oral statement on the directive itself.

While it is too early to provide a comprehensive assessment of how well that directive addresses within its stated scope your subcommittee's recommendations, our review of this directive shows that there is good potential for progress in several of the areas cited in your report.

On the other hand, there may be some other areas that the directive is either silent on or perhaps does not give the kind of emphasis that your committee report recommendations would have enjoyed to have—or preferred to have.

I guess the bottom line of our examination of the directive is that, on the positive side, the directive represents progress by the administration in partially fulfilling the recommendations of your report, your committee report.

However, I think, as was borne out by the previous witnesses, it is not clear whether the directive is the administration's intended mechanism for implementing the recommendations as outlined in your earlier report.

Now, this concern is reinforced, I believe, by the discussions we had with key administration officials. For those who were active in authoring and implementing the directive, which we heard from this morning, it is clear that it was an uphill struggle to get the directive issued in the first place.

And they seem to be somewhat positive, and that may be an understatement, in satisfying the concerns expressed in your subcommittee's report. I would say enthusiastic is the tone I got from the previous witnesses.

Other officials, on the other hand, particularly those who have the traditional responsibility for providing leadership in this very important area, from the discussions we have had, seem to be taking a more or less wait-and-see attitude.

So, the bottom line question here is, whether the directive is or should be the mechanism for dealing with the appropriate safeguards of the national systems across all of Government, or only those with relevance to national security as it is currently defined.

Now, I would like to discuss very briefly two issues that I think are very relevant to this question.

The first issue concerns the lack of definition for unclassified information considered sensitive but relevant to national security; 145 has established a new category, as we have discussed this morning, for information sensitive but unclassified, Government or Government-derived information, the loss of which could adversely affect the national security interests, without clearly defining the information that would be included in this category.

Now, our concern is that if the steering group that Mr. Latham referred to defines this broadly, it could significantly affect the way information contained in computer and telecommunications systems maintained by the civil agencies and by commercial interests must be handled.

For example, unclassified sensitive civil agency information affecting national security interests could include the kinds of systems that I indicate to the immediate right of the dashed line.

The unclassified sensitive information systems not affecting national security is not addressed by the directive itself, and it theoretically could include the kind of systems that we indicate here on the far right of this chart.

Mr. **Glickman**. But theoretically, you could also—theoretically, the former definition, nonclassified sensitive information affecting national security, it is a judgment call, whether any or both of those columns are included, right?

Mr. **Reed**. Exactly, and I am going to comment on that point in my concluding remarks.

Now, we believe that the administration needs to clearly define the types of information that fall under the coverage of 145 and initiate action to address sensitive Government information outside the purview of the directive.

Now, in so doing, the administration should, among other things, clarify when executive agencies must afford the same level of protection against unauthorized disclosure of personal, proprietary and other sensitive information as they do to information classified for purposes of national security.

I might add as a sidelight, as we recommended in one of our earlier reports.

Now, as a second, I think key issue, concerns potential confusion as to who has the responsibility for information security in the Federal Government.

I have already mentioned that the directive establishes a centralized organizational structure, and others have elaborated on this structure this morning.

Now, depending on how broadly or narrowly the directive is applied, the implementation of the directive may lead to confusion as to the responsibility for information security in the Government. In this regard, the term "national security interest" is not defined in the directive, but the clear implication is that the directive is intended to extend to civil agencies information systems.

On the other hand, collectively, OMB, GSA and the Department of Commerce, as Congressman Brooks has highlighted, on the basis of statutory and administrative directives, are responsible for establishing the necessary policies, principal standards that executive agencies must implement to have an efficient and effective information security program.

Now, in contrast, the Directive 145 management hierarchy has similar kinds of authority and responsibility for information systems eventually declared under its purview. Now, this has the potential of leading to confusion in particular among executive agencies having operational responsibility for the systems involved.

Now, in closing, I would like to emphasize that deliberate and constructive resolution of the two issues is needed in determining whether the objectives and recommendations of your earlier report are implemented effectively.

The current course of the administration may preclude such a favorable outcome. For example, if ongoing implementation of the directive results in the administration expanding its scope to address security for the full range of critical national systems, the net effect could cause: First, potential misunderstanding or confusion between responsibilities by existing statutes and those associated with Directive 145.

Second, competing priorities and criteria between military and civilian components for determining appropriate methods for safeguarding information.

And third, raise serious questions about the appropriateness of the management structure established by the Directive 145 for managing effectively such an expanded mission.

If, on the other hand, the directive's addressing of unclassified, sensitive, information relevant to national security is narrowly interpreted, the net effect should minimize the kinds of problems attributed to a broader interpretation.

However, it runs the risk of leaving safeguards for sensitive civilian systems in a vulnerable state, which your 1984 report is trying to avoid.

Now, the bottom line here is that the administration should be encouraged to develop an overt plan of action for resolution of the major issues I have discussed here today, as contrasted to continuing in the direction of prolonged uncertainty regarding their resolution.

Now, that concludes our oral statement, and we would be pleased to answer any of your questions.

Mr. **Glickman**. OK. Thank you, Mr. Reed.

I would like to just have you summarize quickly the key problem areas, again, you see with the directive. I think, No. 1, you said was definitional.

Mr. **Reed**. Yes.

Mr. **Glickman**. What is sensitive, what isn't sensitive——

Mr. **Reed**. That is right.

Mr. **Glickman**. The second problem area was how does this relate to existing laws, whether there is a conflict there, and whether this, in any way, gets us further toward the goal of protecting the kind of information that we had in our committee report.

Mr. **Reed**. Yes, the main issue, the second one that I discussed, the first one clearly was the lack of definition, of what information is within the purview of the directive, and what falls outside of the directive.

The second issue, I did not use the word "conflict," I used the word "confusion."

And what I was alluding to there, principally, was that the responsibilities established by existing statutes for the central agencies, OMB, Department of Commerce and NBS, and GSA and OPM, for example, are very similar to the same sort of responsibilities that have been superimposed by the Directive 145.

And my main point was, depending on how clear those respective responsibilities from both camps are discharged or implemented, the agencies who have to implement the security safeguards could very well be confused.

Mr. **Glickman**. And end up doing nothing or worse than what they would otherwise have done.

Mr. **Reed**. Or tripping over each other.

Mr. **Glickman**. Well, that brings up an interesting point. If, in fact, an agency is faced with compliance with an existing statute, the Brooks Act, something else, to deal with some of these problems, or this directive, which do they follow?

Mr. **Reed**. Well, I will rely on—I will give you a general answer, and then rely on my good counsel here.

As I understand it, for the information—the agency's instructions are—orders are for information that is defined to be under the purview of 145, that for those safeguards attributable to national security, the 145 management hierarchy and authority would prevail.

For any other activities that do not fit in within those—or satisfy those criteria, the existing statutes would more or less prevail.

Would you care to elaborate on that, or perhaps even clarify it, Ray?

Mr. **Wyrsch**. Sure. What Mr. Reed was trying to say was that we do have laws on the books, the Brooks Act, and the Paperwork Reduction Act, and there are very distinct responsibilities that have been placed on these agencies, namely OMB has been given the general oversight authority, if you will, to set government policy.

The Department of Commerce has been given the authority to set standards dealing with the ADP equipment, and administratively, the safeguarding of systems, and GSA has been given the authority under the Brooks Act with respect to the procurement of this equipment.

And what has sort of complicated things, as we see them, is with the issuance of the directive, there has been a similar organizational structure now that has been set up. And it has raised a lot of questions in our minds, and I am sure with everyone else's minds, how does all this relate, in terms of a standard that may be published by the Department of Commerce versus a standard that may be published by, we will say the executive agent, or what have you?

And I don't know if anyone is really in a position to say with any degree of conclusiveness now, on what are the other agencies supposed to do if you have inconsistent or conflicting guidance that may be issued. There have been various pronouncements that have been made by the Secretary of Commerce over the years dealing with ADP standards.

And I believe in terms of NSDD 145, everyone is sort of in a holding pattern now on exactly what are they going to do, because it has yet to be formally implemented in terms of the issuance of any regulations or standards or what have you.

Mr. GLICKMAN. Well, would it be a fair statement until it is clarified this is all going to slow down efforts to provide adequate computer security in various agencies in the United States?

Mr. REED. I don't—well, that perhaps may be an accurate characterization. It clearly will not help, and the critical period is kind of the hiatus period when things are being decided about just what falls under the umbrella and purview of the directive itself.

It is during that period that is very critical, because there is bound to be some confusion until things work out.

Mr. GLICKMAN. Let me ask you this: You are with the GAO, and you are our arm to try to protect at least the interest of Congress. What is the nature of a directive? What is it? Is it better than a regulation? Is it equal to a regulation?

What is its legal status? Does it require any of the notice that a regulation would require? I just want to know how one would characterize what we have here from a legal point of view.

Mr. REED. I am going to ask my counsel here.

Mr. WYRSCH. It is a difficult question to answer in the abstract, a Presidential directive versus a regulation that may be issued by an agency, and I guess it would depend upon the specific area that the directive is being issued in, and in this case, it seems to be in the national interest, which would add great weight to the status of the Presidential directive, compared to the regulation that may be——

Mr. GLICKMAN. Because of the national security interests, is what you are talking about, rather than national interests.

Mr. WYRSCH. Correct.

Mr. GLICKMAN. I mean everything that is done in the government theoretically is in the national interest, you mean national security interests.

Mr. WYRSCH. Correct.

Mr. GLICKMAN. OK.

Mr. WYRSCH. Versus a regulation that may be published by an executive agency, which under normal procedures have to follow the Administrative Procedures Act in terms of prior notice, receiving comments from various sectors of society, et cetera.

In this particular area, for example, the Brooks Act, there is a provision that alludes to the Presidential authority, and Presidential directive, that the authority of the Department of Commerce and GSA that is conferred in that act, there is a provision that explicitly states that their authority is subject to the direction of the President.

Now, I don't think that is to say that the President can arbitrarily displace, completely displace GSA and Commerce, and their regulations, but it does indicate that there is some room that the President can direct those agencies to what they can and cannot do.

Mr. **Glickman**. OK, let me just briefly ask you one final question before I move on to Mr. Lewis.

This National Telecommunications and Information Systems Security Committee has 12—if I go down through the list of members, we have Assistant Secretary of Defense, that was Mr. Latham; and then a voting member from each member of the steering group, which is the Assistant to the President for National Security Affairs, the Secretary of State.

It is roughly represented about half and half, the way I look at it, between military and civilian. Do you have any comments about how this group has been characterized in terms of who are members of it, and whether you think it is a fair and accurate group of people that ought to be on this thing, or do you think that others should be included?

Mr. **Reed**. Well, I have difficulty really giving you an assessment of that question or a direct answer to that question, because the appropriateness of the membership is very difficult to determine until I understand more clearly than I do the scope of the directive, which really should determine the constituency, I think, of the membership.

Now, if the scope is clearly, sort of narrowly interpreted to focus very clearly on national security issues, then that is one thing.

On the other hand, if it turns out to have a very broad interpretation, I very definitely would think that the membership should be expanded beyond what it currently is.

Mr. **Glickman**. OK, and the final question from me is, Are you aware of any coordination that took place between the OMB draft circular on computer security and this directive?

Mr. **Reed**. Yes, I am aware that there was coordination. I am not aware that there was any special kind of coordination between the two parties, that is the 145 people responded to OMB's draft circular just like everyone else did, and the OMB people responded in a coordinative fashion to the 145 directive, just like everyone else was asked to do.

I go, I guess, believe that the views of the people representing the 145 directive are not very positive about the treatment or the extent of treatments, say, that the directive received in the draft circular that deals with computer and telecommunications security.

Mr. **Glickman**. Restate that. I didn't follow you.

Mr. **Reed**. All right. I believe the people that are associated with the directive, the people involved with its implementation and its authorship, and so forth, are a little bit concerned that the directive responsibilities and intentions and so forth did not get very active treatment in the OMB draft circular, which is now being evaluated. And that is all I really know about it, the coordination and extent of coordination that has taken place.

Mr. **Glickman**. Thank you.

Mr. Lewis?

Mr. **Lewis**. Mr. Chairman, I have no questions at this time. Thank you.

[The opening statement of Mr. Lewis follows:]

OPENING STATEMENT
HONORABLE TOM LEWIS
HEARING ON COMPUTER SECURITY POLICY
JUNE 27, 1985

THANK YOU MR. CHAIRMAN.

THE ISSUES THAT WE WILL BE DEALING WITH IN THE HEARING THIS MORINING ARE COMPLEX -- AND GROWING MORE SO. CLEARLY THE PROBLEMS OF PROTECTING SENSITIVE INFORMATION FROM UNAUTHORIZED ACCESS IS BECOMING MORE ACUTE AS THE USE OF COMPUTERS BECOMES MORE WIDESPREAD. VIRTUALLY EVERY FACET OF OUR LIVES IS AFFECTED IN SOME WAY BY THE COMPUTER.

AGENCIES WHO HAVE HISTORICALLY DEALT WITH NATIONAL SECURITY ISSUES HAVE AN AWARENESS OF THE NEED FOR SECURITY AND HAVE DEVELOPED THE TECHNIQUES AND THE EXPERTISE REQUIRED TO PROTECT SENSITIVE INFORMATION. HOWEVER, FOR MANY AGENCIES, THE PROLIFERATION OF COMPUTERS HAS CAUGHT THEM UNPREPARED TO DEAL WITH THE SECURITY REQUIREMENTS ASSOCIATED WITH AUTOMATED INFORMATION SYSTEMS.

THE NEED FOR A COHERENT NATIONAL POLICY ON TELECOMMUNICATION AND AUTOMATED INFORMATION SYSTEMS SECURITY IS CLEAR, AND I BELIEVE IT IS APPROPRIATE THAT THE AGENCY WITH THE EXPERTISE IN HANDLING SECURITY PROBLEMS PROVIDE

SOME GUIDELINES FOR ESTABLISHING THIS POLICY. HOWEVER, SOME LEGITIMATE QUESTIONS HAVE BEEN RAISED CONCERNING THE ROLE OF THE DEFENSE DEPARTMENT IN ESTABLISHING SECURITY POLICY FOR NON-DEFENSE AGENCIES. THESE QUESTIONS NEED TO BE ADDRESSED AND I AM HOPEFUL THAT THE CONCERNS THAT HAVE BEEN EXPRESSED CAN BE PUT TO REST. WE CANNOT LET THESE CONCERNS, HOWEVER SINCERE, LEAD US INTO ENCLESS DEBATE ON THE NEED FOR A COHERENT POLICY ON COMPUTER SECURITY.

THANK YOU, MR. CHAIRMAN.

Mr. **Glickman**. Thank you very much, appreciate your testimony today.

Mr. **Reed**. Our pleasure.

[The prepared statement of Mr. Reed follows:]

U.S. GENERAL ACCOUNTING OFFICE

WASHINGTON, D.C. 20548

FOR RELEASE ON DELIVERY
EXPECTED AT 9:30 A.M., EST
THURSDAY, JUNE 27, 1985

STATEMENT OF

WARREN G. REED

DIRECTOR
INFORMATION MANAGEMENT AND TECHNOLOGY DIVISION

BEFORE THE

SUBCOMMITTEE ON TRANSPORTATION, AVIATION AND MATERIALS
COMMITTEE ON SCIENCE AND TECHNOLOGY
UNITED STATES HOUSE OF REPRESENTATIVES

ON

THE POTENTIAL IMPACT OF NATIONAL SECURITY DECISION DIRECTIVE
(NSDD) 145
ON CIVIL AGENCIES

Mr. Chairman and Members of the Subcommittee:

We are pleased to be here today to discuss the potential impact of National Security Decision Directive (NSDD) 145[1] on civil agencies that are not normally perceived as part of the national security establishment. We will also provide a status report on how well the directive addresses recommendations made by this Subcommittee in its April 1984 report on computer security and privacy.[2] I have with me Mr. William Franklin, Associate Director, and Dr. Harold Podell, Group Director, from the Information Management and Technology Division and Mr. Raymond Wyrsch, Senior Attorney from our Office of General Counsel.

On October 17, 1983, I testified before your Subcommittee on problems that we found in executive agencies concerning inadequate federal information security policy. In particular, I stressed the need for revising federal guidance and included a recommendation to specify when executive agencies must provide the same level of protection for sensitive information as they do for information classified for national security.

In preparing for this testimony, we had discussions with government officials who had key roles in authoring and implementing the directive being examined today. We also drew, to a limited extent, from our on-going work for your Subcommittee that addresses the security status of major information systems. Our principal basis for examining this directive was your 1984 report.

---

[1] NSDD 145, National Policy on Telecommunications and Automated Information Systems Security, dated September 17, 1984.

[2] Computer and Communications Security and Privacy; April 1984 report prepared by the Subcommittee on Transportation, Aviation and Materials, House Committee on Science and Technology.

In that report, you expressed concern that both public and private computer and telecommunications systems associated with such areas as banking, entitlement programs, law enforcement, and industrial processes need additional protection along the lines that the defense establishment has traditionally provided for its national security information. Such additional protection requires an appropriate mixture of physical, technical, and administrative security measures.

You also highlighted a lack of central leadership in establishing national policies for the protection of critical national systems of government. Specifically, you noted weaknesses in federal policy for computer and telecommunications security. OMB and other central agencies, who traditionally have had this responsibility, were chided for falling short in security management. In reinforcing your concern, you cited a variety of weaknesses associated with safeguarding these key computer and telecommunications systems. Inadequacies were noted in such areas as research and development, measures to prevent unauthorized access to critical systems, personnel training, and a data classification structure for non-national security data, etc.

Your report culminated in a variety of recommendations to Congress and the Administration, which were intended to strengthen federal leadership. The recommendation to the Congress called for the establishment of a National Commission to examine the legal, economic, institutional, social, and technical aspects of safeguarding computerized resources and other key issues. The Congress has not yet acted on this recommendation.

Recommendations to the Administration generally called for an immediate assessment and analysis of problems associated with critical national systems, as well as a strengthening of the organizational arrangements, so that national policies could be developed and implemented to ensure appropriate safeguards for critical national systems.

Executive actions related to Subcommittee report recommendations

Two independent Administration initiatives, both of which were started before the Subcommittee's April 1984 report, address several Subcommittee report recommendations.

First, the Department of Defense (DOD) developed NSDD 145, which was signed by the President and issued on September 17, 1984. The NSDD objectives include "assuring the security of telecommunications and automated information systems which process and communicate classified national security information, and other sensitive government national security information, and offering assistance in the protection of certain private sector informaation." This initiative established an organizational structure to guide the conduct of national activities directed toward safeguarding such systems.

This structure consists of four organizational components. The Systems Security Steering Group, which is responsible for overseeing the directive and ensuring its implementation, is chaired by the Assistant to the President for National Security Affairs and has six Administration department or agency heads. The second component, the National Telecommunications and Information Systems Security Committee (NTISSC), is chaired by the Assistant Secretary of Defense (Command, Control, Communications and Intelligence-C3I). This committee was established to operate under the direction of the Steering Group to consider technical matters and develop operating policies as necessary to implement NSDD 145. The NTISSC has 22 members, of which 10 are from DOD agencies. The third component is the Executive Agent for the Government for Telecommunications and Automated Information Systems Security (in this case, the Secretary of Defense). The Executive Agent acts in accordance with policies and procedures established by the Steering Group and the NTISSC. The fourth component is the National Manager for Telecommunications Security and Automated Information Systems Security (in this case, the Director of the National Security Agency). The National Manager is responsible to the Secretary of Defense as Executive Agent for carrying out the Executive Agent's responsibilities. Attachment I lists the members of the various components.

The remaining Executive Branch initiative was an effort by the Office of Management and Budget (OMB) to consolidate and update four existing circulars pertaining to the management of federal information resources, including computer and telecommunications security. This draft circular, released for public comment on March 15, 1985, is intended to further implement various statutory and administrative provisions and policies concerning general information policy, information technology, security, privacy, and maintenance of federal records. OMB is now evaluating the comments that it has received.

Our testimony will focus on the degree to which NSDD 145 satisfies the requirements specified in the Subcommittee report and the potential impact of NSDD 145 on civil agencies.

NSDD 145 is a move in the right direction

While it is too early to provide a comprehensive assessment of how well NSDD 145 addresses, within its stated scope, the Subcommittee's recommendations, our review of this directive shows there is good potential for progress in several of the areas cited in your report. For example, a rather elaborate organizational structure has been established at high levels. The NSDD 145 organizational structure is charged with the responsibility for setting policy, providing direction, leadership, and guidance to executive agencies, increased research and development support, etc. Our review also shows that the scope of the directive falls short or is silent concerning some of the areas in your 1984 report, such as training and security awareness and computer abuse reporting.

I now would like to briefly discuss the extent to which NSDD 145 addresses the Subcommittee report's recommendations.

Federal leadership. The Subcommittee report recommended that the Administration "begin an immediate assessment of the problems and issues in order to develop a set of national policies that will ensure the protection of critical national systems relevant to government, industry, commerce, and the society." NSDD 145 partially fulfills the federal leadership recommendation by creating a single organizational entity responsible for policy, direction, and technical leadership relative to the protection of unclassified sensitive data that could affect national security. However, this directive does not cover information in national systems that is sensitive but is not considered critical to national security.

Technical and administrative guidance to federal agencies. The Subcommittee report recommended that "OMB should establish a central focus to provide technical assistance to agencies that are responsible for sensitive, non-national security data in selecting tools and techniques to protect their computer systems....General Services Administration should consider developing a manual to provide agencies with administrative guidance...." While the Subcommittee recommendation contemplated that OMB and the General Services Administration (GSA) would provide technical assistance, NSDD 145 has, in part, addressed this recommendation. Specifically it requires that telecommunications and automated system security guidance be provided to governmental departments and agencies. It does not, however, specifically cover the administrative guidance needed to complement the technical procedures.

Research and development. The Subcommittee report encouraged expanded research efforts to identify vulnerabilities that may affect future systems. NSDD 145, through the responsibilities granted the Executive Agent of the Government for Telecommunications and Automated Information Systems Security, supports the intent of the Subcommittee recommendation. In particular, the directive states, the Executive Agent should "act in accordance with policies and procedures established by the Steering Group and the

NTISSC to...conduct, approve, or endorse research and development of techniques and equipment for telecommunications and automated information systems security for national security information."

Certification of systems. The Subcommittee report identified a need for certification of hardware and software to determine their adequacy in providing the appropriate level of security. NSDD 145 gives the National Manager the responsibility to "operate a central technical center to evaluate and certify the security of telecommunications systems and automated information systems...as well as...enter into agreements for the procurement of technical security material and other equipment, and their provision to government agencies and, where appropriate, to private organizations, including government contractors, and foreign governments."

Non-national security data classification. The Subcommittee report recommended consideration of the advantages of establishing a non-national security data classification structure, such as critical sensitive, sensitive, and non-sensitive "to protect certain categories of sensitive data (e.g., financial, medical, inventory systems, etc.) in the Federal Government." Although NSDD 145 does not specifically address the data classification issue, we are aware of working groups created as a result of NSDD 145 to address key issues, such as a classification structure for sensitive data, which affects the national security interest.

The three Subcommittee report recommendations that are not specifically addressed by the directive concern (1) threats and vulnerabilities, (2) training and security awareness, and (3) computer abuse reporting. However, depending on how NSDD 145 is implemented, these recommendations could be partially addressed by actions taken under the previously discussed recommendations.

On the positive side, the NSDD 145 initiative represents progress by the Administration in partially fulfilling the intended purpose of your report through the institution of improved management mechanisms. However, it is not clear whether NSDD 145 is intended to be the Administration's mechanism for implementing recommendations of your report. This concern is reinforced by discussions we had with key Administration officials. For those who were active in authoring and implementing NSDD 145, it's clear that it was an uphill struggle to get the directive issued in the first place, and they seemed to be somewhat positive in satisfying the concerns expressed in your Subcommittee report. Other officials, particularly those who have the traditional responsibility for providing leadership in this very important area, seem to be taking a "wait-and-see" attitude. So, the bottom-line question here is whether NSDD 145 is or should be the mechanism for dealing with appropriate safeguards of national systems across all of government or only those with relevance to national security as it is currently intended. Now I would like to discuss two issues that are relevant to this question.

ISSUES REQUIRING CLARIFICATION

The first issue concerns a lack of definition for unclassified information considered sensitive with a national security interest and sensitive information that does not affect national security.

My second concern is the potential confusion as to the responsibility for computer and telecommunications security management in the federal government.

Scope of NSDD 145 Unclear

NSDD 145 has established a new category of information "sensitive, but unclassified, government or government-derived information, the loss of which could adversely affect the national security interest..." without clearly defining the types of information that would be included in this category. Our concern is that if the Steering Group defines this broadly it could significantly affect the way information contained in computer and telecommunications systems maintained by civil agencies and by commercial interests must be handled. For example, unclassified sensitive civil agency information affecting national security interests could include hazardous materials information held by the Department of Transportation, flight safety information held by the Federal Aviation Administration, and monetary policy information held by the Federal Reserve.

Unclassified sensitive information not affecting national security is not addressed by NSDD 145, although it was never intended to do so and we are not necessarily advocating NSDD 145 do so. Information in this category could include such items as earnings and beneficiary information held by the Social Security Administration and financial information held by the Securities and Exchange Commission.

We believe that the Administration needs to clearly define the types of information that fall under the coverage of NSDD 145 and initiate action to address sensitive government information outside the purview of NSDD 145. In so doing, the Administration should, among other things, "clarify when executive agencies must afford the same level of protection against unauthorized disclosure of personal, proprietary, and other sensitive information as they do to information classified for purposes of national security," as recommended by GAO in 1982.[3]

Potential for confusion as to who has the responsibility for information security in the government

NSDD 145 establishes a centralized organizational structure with designated responsibilities for policy development and implementation for telecommunications and automated information systems that process classified national security information and other sensitive information. Compromising this information could affect national security.

Depending upon how broadly or narrowly NSDD 145 is applied, the implementation of the directive may lead to confusion as to the responsibility for information security in the government. In this regard, the term "national security interest" is not defined in the directive, but the clear implication is that the directive is intended to extend to civil agencies' information systems.

On the other hand, collectively, OMB, GSA, and the Department of Commerce, on the basis of statutory and administrative directive, are responsible for establishing the necessary policies, principles, standards, and guidelines that executive agencies must implement to have an efficient and effective information security program.

---

[3] GAO report Federal Information Systems Remain Highly Vulnerable To Fraudulent, Wasteful, Abusive, And Illegal Practices, (MASAD-82-18, dated Apr. 21, 1982).

Let me give you two examples where confusion over agency responsibilities may arise. First, the Brooks Act (40 U.S.C. 759) gave OMB general oversight responsibility over Commerce and GSA activities in carrying out their respective responsibilities. In 1978 OMB issued OMB Circular No. A-71, Transmittal Memorandum No. 1,[4] setting forth the responsibilities for the development and implementation of computer security programs by executive agencies. The Paperwork Reduction Act of 1980 (44 U.S.C. 3504) broadened OMB's information security program responsibilities as part of its leadership role in information resources management (IRM).

In contrast, NSDD 145 sets up a Systems Security Steering Group to act as the central organization to oversee the implementation of this directive. We are concerned that in implementing this leadership responsibility, the Steering Group could issue policy that creates questions in regard to OMB's responsibility for federal IRM leadership.

Second, the National Bureau of Standards (NBS) is responsible for developing and issuing computer security standards and guidelines. In contrast, NSDD 145 gives the Executive Agent the authority for approving and providing minimum security standards for telecommunications and automated information systems. Further, the directive requires NBS to submit all security-related standards and guidance affecting national security to the Steering Group for review and approval.

---

[4] Security of Federal Automated Information Systems, Circular No. A-71, Transmittal Memorandum No. 1, dated July 27, 1978.

SUMMARY AND OBSERVATIONS

NSDD 145 is a positive step for establishing a policy framework for the protection of classified and sensitive information affecting national security and is in line with the major thrust of the Subcommittee report, as it relates to sensitive, unclassified information with a national security interest.

There is also an area of information outside the scope of NSDD 145 which must be addressed. This is sensitive information without a national security impact. Determining the appropriate mechanism for addressing this information involves tradeoffs among economic, political, and social implications, such as the impact of security measures on agencies' ability to freely exchange information in support of their missions.

If resolution of this issue favors expanding the scope of NSDD 145 to cover the full range of critical systems, then the Administration must be sensitive to political and social concerns that are likely to be expressed by government, as well as non-government, entities. The number of military organizations represented on the NTISSC and related subcommittees could cause complications, given the traditional notion that the military should not unnecessarily interfere with civilian agency operations. Irrespective of the approach taken, implementation actions must be adjusted to ensure the spirit of the Subcommittee report recommendations is being covered or addressed.

Regardless of how the above issue is resolved, potential confusion may result due to other existing executive agency organizational responsibilities established by laws and regulations.

Our on-going work examining the status of security problems in the civil agencies, reinforces the need to protect critical national systems identified in your 1984 report. It's not clear whether the administration has pinpointed your recommendations as a target objective.

In conclusion, the Administration is aggressively pursuing the protection of information related to national security and in a sense seems to be waiting to see if the NSDD 145 initiatives will address other issues emphasized in your 1984 report. This could be a high risk approach towards achieving the objectives of your Subcommittee report.

- - - - -

This completes my prepared statement. We would be pleased to answer any questions.

ORGANIZATIONAL STRUCTURE ESTABLISHED BY NSDD 145--
NATIONAL POLICY ON TELECOMMUNICATIONS
AND AUTOMATED INFORMATION SYSTEMS SECURITY

The Systems Security Steering Group

- --The Assistant to the President for National Security Affairs, Chairman
- --The Secretary of State
- --The Secretary of Treasury
- --The Secretary of Defense
- --The Attorney General
- --The Director of the Office of Management and Budget
- --The Director of Central Intelligence

The National Telecommunications and Information Systems Security Committee (NTISSC)

- --Assistant Secretary of Defense (Command, Control, Communications and Intelligence--C3I), Chairman
- --Voting representative of each member of the Steering Group

--The Secretary of Commerce

--The Secretary of Transportation

--The Secretary of Energy

--Chairman, Joint Chiefs of Staff

--Administrator, General Services Administration

--Director, Federal Bureau of Investigation

--Director, Federal Emergency Management Agency

--The Chief of Staff, United States Army

--The Chief of Naval Operations

--The Chief of Staff, United States Air Force

--Commandant, United States Marine Corps

--Director, Defense Intelligence Agency

--Director, National Security Agency

--Manager, National Communications System

The Executive Agent of the Government for Telecommunications and Automated Information Systems Security

--The Secretary of Defense

The National Manager for Telecommunications Security and Automated Information Systems Security

--The Director, National Security Agency

Mr. **Glickman**. We have two more sets of witnesses. Our next witness is Mr. Jerry Berman and Mr. Allan Adler, legislative counsels for the American Civil Liberties Union.

I might just mention for the record that the GAO is doing a report card on, so to speak, activities by each Federal agency, how they are doing in the computer security area, and we will have that report sometime during the fall.

It is a pleasure to have you gentlemen here. You have a fairly short prepared statement. You may read it or summarize it as you desire.

STATEMENTS OF JERRY BERMAN AND ALLAN ADLER, LEGISLATIVE COUNSELS, AMERICAN CIVIL LIBERTIES UNION, WASHINGTON, DC

Mr. **Berman**. Mr. Chairman, I am Jerry Berman with the ACLU, and to my right is Allan Adler. Rather than summarizing our statement, I think we would like to just comment on some of the concerns here.

What Allan will describe when we turn to him, is the shift from a focus of the National Security Agency and the Government on protecting information in the national security area, to a sweeping concern with information in the civilian sector.

While there is certainly concern about the vulnerability of those systems, and we don't want to underestimate the threat to those systems, there are grave questions about making the National Security Agency the lead agency.

And I think that to understand this is to realize what kind of an agency it is, so that we know when we create policy and conduct oversight in the Congress, that other values will be taken into account.

The National Security Agency, contrary to what Mr. Deeley claims, is not a "national service" agency. He tried to give us this impression that it was somehow created as a national service by President Truman in 1952.

The National Security Agency is a security agency. If you will, it is a national spy agency, and a very good one. It has great technical capability and knowledge and expertise, as Mr. Deeley pointed out. But, as Frank Church, the late Senator from Idaho said in conducting the Church committee hearings in the late 1970's, it also has the technical capabilities which if turned on the American people would eviscerate the right of privacy. We would have nowhere to hide.

And as we must remember, while it performs technical services for the Government and is driven by national policy goals, in the late and midseventies, it was driven by concerns about the alleged foreign connections of antiwar and civil rights activists, and was asked actively and complied with agencies' requests to watch, list, and to intercept the international communications of thousands of American citizens, and for 30 years, was collecting all of the international telegrams of American citizens on a routine basis.

Those things have come to a halt, but it is an agency which thinks in terms of security. Its mission is security. So when we are talking on the civilian side of the Government, when we are talking about health and human services records, as Mr. Latham did this morning, as possibly within the purview of sensitive information in need of protecting, there are serious questions, even for a privacy advocate like myself, of having the National Security Agency sort out how HHS is going to conduct its business to protect that information.

This is an omen where policy demands not only that we concern ourselves with security, but our traditional openness in Government, privacy concerns, trust of Federal employees, the whole way that we do business in an open society and a democratic government.

I am not saying that the National Security Agency is a totalitarian agency, but its mission is to tell agencies of Government how to keep things secret. What we find lacking in this whole directive is any counterbalancing representation or measures which allow these other values to have weighed in the process that has been developed under NSDD 145.

The Congressman asked what was the legal States of national security directives versus Executive orders? National security directives are used because they do not come under the Administrative Practices Act. The administration can avoid public comment, avoid publication in the Federal Register, avoid direct Presidential accountability. And so, it allows policy to be made which may be very sensitive policy, largely outside the purview of Congress, without congressional oversight, and so forth.

After Mr. Adler describes the sweep of information that may be protected through communications and computer systems under this directive, I would like to come back and suggest and almost urge that Congress call a moratorium to this process and start to develop some countervailing measures and oversight mechanisms to ensure that we properly weigh openness and privacy considerations in the implementation of this very important policy.

Mr. ADLER. As we have suggested, if there is a pervasive theory in NSDD 145, that underscores our concerns, it is the view that national security information goes far beyond the President's Executive order on national security information, which provide procedures, standards, and criteria for classification, to encompass what, in our view, is a seemingly unbounded range of nonclassified information in civilian operations in both the public and private sectors.

I think it is very important to understand this in the context of some of the proposals, initiatives, and policies that the administration has followed over the past 4½ years. Beginning with the issuance of Executive Order 12356, which was President Reagan's Executive order on classification policy superseding President Carter's Executive order, there has been a deliberate, calculated effort to try to expand the realm of what can be considered "national security" information.

The purpose of that expansion is to try to promote greater government control over information, and the best way that can be done is if the information can fall within the "national security" rubric.

Otherwise, various statutory restrictions on the President's authority in this area prevent him from asserting the kind of control that the executive branch would prefer.

At the time Executive Order 12356 was still in draft form, successive drafts ultimately leaked to the newspapers, thereby precipitating hearings in the House Government Operations Committee.

What the administration was attempting to do, for the first time, was to create a fourth level of classification, something that came below top secret, secret and confidential.

Realizing that there was a tremendous amount of information that they wanted to control that could not clearly be considered as classifiable "national security information," they wanted to try to reach a broad category of information under the standard that loss of such information or unauthorized disclosure of such information could cause a loss of economic or technological advantage to the United States, an impossible standard to define, and a standard which, if you did define it literally, would encompass just about any kind of information that the Government and the public sector deals with.

The fourth level of classification was rejected, it became too controversial and they weren't able to accomplish that. So instead, in issuing Executive Order 12356, President Reagan made several changes from the Carter order, as well as changes even from the predecessor Nixon Executive order, which in the view of the ACLU and in the view of the House Government Operations Committee, did absolutely nothing to address the massive problem of overclassification in government, but in fact, led to the probability that more information would be classified as national security information.

For one thing, the Reagan Executive order removed the standard qualification that information, in order to be classified, had to be expected to cause identifiable damage to national security. That term, "identifiable," was eliminated.

The Reagan administration argued they were trying to deal with a problem involving FOI litigation. But the truth of the matter is that by eliminating that standard of identifiable damage, you provide a situation where classification could be accomplished without having to actually articulate and explain how the information fit into any legitimate scheme of national security interests.

At the same time, the Executive order eliminated the discretion not to classify information which arguably would qualify for classification. This was done by eliminating the requirement in President Carter's Executive order that even if information qualifies for classification, before it is classified or before classification is maintained, you would have to consider the public interest in disclosure of that information.

And if the public interest was overriding, declassify it regardless of its qualification for classification.

The same thing was true with respect to the addition of a new category of classifiable information relating to vulnerabilities in systems and programs related to national security. That is the catch-all. It is rather difficult to think of any information that the administration would not argue in some fashion falls within that category.

And by the same token, the President, in his Executive order, for the first time provided explicit authority to reclassify information that had been previously declassified and released by the government.

Once it had gone as far as it could with the Executive order on classification, the Reagan administration sponsored several statutes which, unfortunately, have been enacted by Congress, that take information manifestly unclassifiable and, nevertheless, put it beyond public reach in terms of access under the Freedom of Information Act, and in addition, provide criminal penalties for unauthorized disclosure.

One such measure, was a provision in the 1981 Department of Energy National Security Program authorization bill, that created the rather interesting category of information called unclassified controlled nuclear information.

Similarly, several years later, the Department of Defense was able to obtain a statute that gives it the authority to withhold from public release any technical data, with military or space application, that is subject to the export control laws.

Now, as you all know, the export control system has been a major subject of controversy in Congress over the past two sessions, primarily because it has generally been agreed that far too much technology, and therefore, far too much technical data is regarded as controllable by the Government.

This has had a very repressive impact, particularly in the area of academic research, which many people regard as the wellspring of the technological superiority that not only keeps the United States economically strong, but also strong as a power in national defense.

The result has been visa restrictions on foreign nationals who come to the United States because of concern that they will acquire unclassified but export-controlled information; scientific papers presented at meetings and conferences in the academic community, and by professional scientific associations, have been pulled from public presentation at the request and initiation of the Defense Department, on the grounds that they would disclose unclassified but export-controlled technical data.

And at the same time, there have even been restrictions placed upon university course selections and what courses foreign students at American universities can attend.

Mr. GLICKMAN. Mr. Adler, I am going to have to ask you to stop. We are in the middle of a vote, and we will come back in about 15 minutes, so just wait there. We will be back in about 15 minutes, and then we have one other witness after you.

[Recess.]

Mr. GLICKMAN. Why don't you proceed, continue where you were.

Mr. ADLER. Thank you, Mr. Chairman.

The point that I was just trying to make by going through the history of the Reagan administration's policies in the area of expanding national security information, is that our concern about the lack of definitions in this directive is very real.

It is grounded in policies that we have seen come into effect as law, which are already having a very detrimental effect on the ability of the public to examine a number of very important programs of the U.S. Government concerning nuclear power and defense research and development, just to give you two examples.

The other point that I want to make is that the means chosen to protect information often involves a judgment based upon the kind of information that you are trying to protect, and this administration has seen fit to propose various means of protecting information that have proven to be quite controversial. In our view, some of them were flatly unconstitutional.

You have already heard, as Mr. Brooks told you, about the polygraph, but for example, there was another NSDD, NSDD 84, which proposed widespread use of lifetime secrecy and censorship agreements for all Government employees who have access to a kind of classified information known as SCI.

According to the GAO reports, this would affect more than 150,000 individuals in the Defense Department alone. At the same time, the administration has made increasing use, and I might add, rather abusive use of the security background investigation.

I will give you two very good examples of this. There have recently been lawsuits involving the Department of Education and the Library of Congress, situations where individuals who had absolutely no access to classified information were nevertheless required to undergo full background investigations by the FBI for reasons which were never clearly articulated by the Government.

The general notion was that the administration wanted to be certain of the trustworthiness of these individuals, even though they had no access to classified information, because of the positions they occupied. That is not the purpose of a background investigation, unless you are dealing with classified information.

The same thing is true with respect to administration policies and programs attempting to limit press contacts with Government employees, based upon the mistaken belief that Government employees ordinarily blurt out classified information, or even that when they are discussing information that is not at all classified, nevertheless the government should be able to a control what information is given to the press.

The primary example, though, that I want to give has already been mentioned. And that is, the Computer Fraud and Abuse Act of 1985, that was enacted in the continuing resolution just before the end of the last Congress.

Here, I think is the clearest example of an attempt to secure information by means which could distort the assessment of the need to secure information in the first place.

The Computer Fraud and Abuse Act was originally intended to create Federal criminal jurisdiction over computer hackers, people who entered computer data bases without authorization. There is a provision in the Computer Fraud and Abuse Act that does, in fact, create a criminal offense for those who enter a Government computer data base without authorized access.

There is another provision, however, which creates criminal liability for individuals who have authorized access to enter a computer data base, but having had such access, use or disclose information to for a purpose to which such authorization does not extend.

In effect, what the statute now does is create criminal liability for disclosure of information which would not warrant such protection except for the fact that the information is in a government computer data base.

If you disclose exactly the same information from a paper file, since it might be available to you under the Freedom of Information Act, absolutely no criminal or civil liability would adhere. But because the information is in a computer data base, that fact alone raises criminal liability under this statute.

So, we are very concerned, indeed, that if you place NSA, with its basic national security mindset, in charge of developing security for the systems of all civilian agencies of the Government and in position to influence the protection of systems in the private section, what you are going to find is that you will not only have an effect on the means by which information is secured, but you will have a changing characterization of the need to protect particular information that not be justified by the nature of the information.

Mr. BERMAN. Let me just come back to what I think we would like to talk about, in terms of recommendations.

What we see is information policy being made by the Government largely without congressional oversight, at least coherent congressional oversight.

NSA, we spent a lot of time in the mid-seventies trying to create the House and Senate Intelligence Committees, which has a certain kind of jurisdiction, but is not exactly a public forum for discussing these kinds of issues, control over civilian agencies, setting policy for civilian agency Government information.

The Judiciary Committee has one set of concerns. This committee has another set. House Government Operations has its concerns. But falling between the cracks is the whole development and implementation of information policy in the ongoing process of bureaucracy.

So that unless Congress can find a way to intervene in this process in some coherent way, I think that the horse is out of the barn and we are just kind of recording history here.

Mr. GLICKMAN. Let me ask you a question: What you are basically saying, or maybe it is how I am reading it, is that you take something which, under maybe traditional thinking, might be a regulation, and you just call it a national security directive, and by doing that, you avoid the Administrative Procedures Act, all public notification requirements, and even appropriate input from other agencies of Government.

Mr. BERMAN. That is absolutely right. And I think that is what has happened here. It also takes the President a step away from accountability for—by making it a directive rather than order there is some blurring of what exactly is the administration's role—it doesn't draw the attention of the press and the Congress——

Mr. GLICKMAN. Now, you will have to maybe edify me a bit. Quickly, tell me the legal difference between an order and a directive.

Mr. BERMAN. We don't know. I really don't think it has been litigated or settled.

Mr. ADLER. The primary difference in terms of practical impact is that when a President issues an Executive order, it is published in the Federal Register, and so, many more people know about it, and the press is much more aware of it.

Mr. **GLICKMAN**. But there is no requirement for public comment. An Executive order is an Executive order, right? I mean, it doesn't have to go through any, other than the notice requirements——

Mr. **ADLER**. It has the force of law equal to a statute.

Mr. **GLICKMAN**. But it doesn't have the requirements for public review, comment or anything else. It has the force of statute in a sense, but it is just there, and it is in the Federal Register so you can see it.

Mr. **BERMAN**. Exactly.

Mr. **GLICKMAN**. But a directive is just kind of issued and people see it, but not in any formal way.

Mr. **BERMAN**. I think that is at least the process impact of a directive, but what I was saying is, I am not sure what the legal impact is. For example, if the President under this directive instructed that a series of break-ins be conducted, whether that would have the impact of law versus an Executive order——

Mr. **GLICKMAN**. Well, that is one of the things the GAO talked about was what are the effects of conflicting and competing statutes. I mean, to some extent, this subcommittee, I think, has something to do, I don't know about with the directive, because I certainly wouldn't have done it that way, but we have been pushing this issue for a long time, we think that there is significant breaches of security in Federal agencies, and we think that—my concern has been more on the civilian side of the picture, and we think that information stored in computers is not protected. It is subject to abuse.

And we have been pushing the agencies to move on it, and we have had OMB here before, they have issued some form of directive in this area of their own, not the same kind of directive, and now, we see this.

I would hate to have seen the defense community use our hearings as a rationale to deal with the issue in a way that may not have provided adequate public notice and comment into the process.

I also am aware, however, that the NSA does have some experience in cryptography and in other techniques that the civilian agencies ought to be able to go to and utilize.

Mr. **BERMAN**. Absolutely. I tried to make the point, I think you were called away for a moment, that we are not saying that NSA does not have a role here, that they have great technical expertise, and they know how to secure information.

It is simply that there are other issues and other values that have to be weighed in that process, and NSA—let me speak more broadly. When you talk about the composition of the steering committee, it is weighted in terms of the military agencies.

And we see no mention in NSDD 145 that security be conducted consistent with open government, consistent with privacy concerns. There is no recognition that those values might have to be taken into account.

And so, rather than beating NSA on the head, it is really the whole way that the issue is being framed that is the issue, and we think that part of the answer is more coherent oversight by the

Congress. One possibility is a Select Committee on Information and Communications Security, which would bring together the various jurisdictions just for a couple of years, to watch the implementation of this process, and also to think about the need for legislation. Another is to require that NSA, if it wants to come out of the closet or out of the cold, to use the LeCarre metaphor, then it ought to have a legislated charter. The NSA was for a charter under the Carter administration which would bring it out from secrecy and spell out it's responsibilities and set some limitations on the agency.

And this directive , I think, ought to be put into statutory form. The Congress, I think, given the current climate, would have to demand that the administration weigh other concerns such as openness and privacy in statutory language.

I mean, you can't just tell this administration, be concerned about privacy, because they don't take it seriously, and we could go into long statistics about how it has cut back oversight in that area.

But Congress should say: We want secure communications and computer systems, but we want it done in a balanced way, and so we are going to set some criteria up, expand this committee, propose legislation, have oversight, and watch it with some care.

And unless that is done, I think that the hearings will be of interest, but that this process will move much, much too quickly.

Mr. **Glickman**. OK, thank you.

Mr. **Berman**. Thank you.

Mr. **Glickman**. Mr. Lewis?

Mr. **Lewis**. Thank you, Mr. Chairman.

Do either of you gentlemen that there are data that are not classified and yet are sensitive and should be protected?

Mr. **Adler**. Certainly, we do. Our main concern is that the decision to decide what unclassified information requires protection, what degree of protection it requires, and what means will be used to insure protection, should be done in an open, deliberate fashion by Congress, and not by executive fiat.

Mr. **Berman**. I have a slightly narrower view.

Mr. **Lewis**. It figures.

Mr. **Berman**. I can think of lots of information which we could make an argument is sensitive and could cause damage to national security whether it is information about grain shipments or information down at the Commerce Department about which way the economy is going. There are labor statistics which would tell a foreign power or a foreign government or the Soviets which way our economy is moving.

But unless we stay within the limits of identifiable damage to national security as the cutoff point for classified of information, I think you potentially make much of the information in the government "sensitive" and therefore subject to restricted access.

Every agency will tell you that its information is very sensitive. I think we would be on a real slippery slope having lost any definition of what "secret" means. We would move very swiftly away from an open government system.

It is not that I can't perceive of sensitive information, but it can be defined very broadly.

Mr. **Lewis**. That is what I want to get to. How do you suggest we deal with the basic conflict between the people's right to know and the people's right to privacy?

Mr. **Adler**. I would say that the ACLU has to deal with that all the time, because as you know, we do have a great deal of concern about the public's right to know what the Government is doing, and because the Government does contain in its records a great deal of information relating to the personal lives of individuals.

We are also very concerned about personal privacy. It is a balancing process.

Mr. **Lewis**. How do you do that? How do you know which is most important, and which should take precedence?

Mr. **Adler**. It is a case-by-case matter, for the most part.

Mr. **Berman**. I think it is going to have to be debated. For example, if Congress proposed legislation instead of this directive, in which it was attempting to define protection for sensitive information——

Mr. **Berman**. Then we would—in public hearings—find out what different agencies thought fit in that class Congress would create a legislative history about what, outside of classified information, fit into that category. At least we would have the agencies coming in and saying, "Well, we will tell you what we think is sensitive, it is crop information over at Agriculture, it is social security records over at HHS."

And the Congress would begin to identify what at least the bureaucracy is thinking about, and then others can come in and debate and say, "That is much too broad." Or this is going to destroy open government. We could at least have a debate and begin to define the scope of sensitive information.

What we are now talking about is terribly abstract.

We don't know what they are talking about, so we are very concerned, and maybe more paranoid than we ought to be, but certainly they haven't come forward and said:

> We can tell you the boundaries and whether or not we are going to create compartmentalized need-to-know requirements then Social Security Administration information. We don't know.

So, I think that maybe it is hedging, but it is only Congress, I think, that is in a position to at least have the dimensions of sensitive information debated in a public forum.

Mr. **Adler**. Let me also suggest to you that in the past, Congress, unfortunately, also has played a role in seeing that decisions about what kind of information is considered to be sensitive are not made in a public forum.

The two examples that I gave you of the Department of Energy's UCNI statute, and the Department of Defense's statutory authority to deny public access to certain technical data, both provisions were enacted as riders on authorization bills.

There were no hearings held on the questions of why such information was sensitive, what was being described within the category of information to be withheld under this statute, and why, in fact, such information presented such dangers to justify withholding from public access.

There were never public hearings on it, the measures were never introduced as individual freestanding bills to be discussed as such. They were simply added as riders onto authorization bills.

Our concern, therefore, is that Congress also should share the responsibility of ensuring that these kinds of decisions are made in a deliberate and open fashion, where there is time to debate the need to protect certain information.

Mr. LEWIS. Well, Mr. Chairman, I guess we could debate this a little bit longer, but I think—I would like to ask one question that is off the record—a little off the hearing—but what is your opinion of the news blackout by the administration on the hostages?

Are you for or against that?

Mr. BERMAN. We are against it.

Mr. LEWIS. That is what I thought. OK.

Mr. BERMAN. I can give you an explanation. I think you would expect it, I believe that the press has a duty to report the news, and it is news, and certainly I think it is subject to being—one press is subject to being manipulated and so forth, but even during the Iranian crisis, I think the press played—kept some things secret when they needed to be kept secret, and I think it is easier to get their voluntary cooperation in trying to handle these situations than to try and impose a news blackout, in violation of the first amendment.

[The prepared statements of Mr. Adler and Mr. Berman follow:]

Statement of

Allan Robert Adler and Jerry J. Berman
Legislative Counsel
American Civil Liberties Union

on

National Security Decision Directive 145

before the

Sub-committee on Transportation, Aviation and Materials

Committee on Science and Technology

U.S. House of Representatives

June 27, 1985

Mr. Chairman and Members of the Subcommittee:

On behalf of the American Civil Liberties Union, we want to thank you for the invitation to appear here today to discuss the implementation of President Reagan's National Security Decision Directive 145 concerning National Policy on Telecommunications and Automated Information Systems Security.

It is no secret that increasing reports of computer-related fraud and abuse, together with detailed press accounts of the alleged espionage activities of present and former members of the military and intelligence establishments, have generated broad new concerns about the ability to protect telecommunications and automated information systems, in both the public and private sectors, against serious threats of exploitation and compromise.

The ACLU is sympathetic to these concerns because it has long been a champion of both the public's right to obtain necessary information from the Government, and the individual's right to protect his or her personal privacy from unwarranted intrusion or exposure by the Government. Although these vital interests in openness and confidentiality can often appear in conflict, it is clear that neither can be properly served in the present climate where a generalized perception of systemic information security weaknesses is not only undermining routine assurances of effective protection for legitimate confidentiality interests but may well be leading to overreactive remedial programs that could result in unnecessary and undesirable new secrecy practices.

Numerous initiatives, proposals and pronouncements of the Reagan Administration over the past four and one-half years have demonstrated its firm inclination to view all government information policies through the dark, uneven filter of what it broadly defines as "national security interests." It is thus not surprising that in NSDD 145, issued by President Reagan on September 17, 1984, the White House has established a "comprehensive and coordinated approach" to telecommunications and automated information systems (T&AIS) security issues that casts its "Objectives" and "Policies" in the vague terms of those interests, and attempts to meld civilian systems, handling nonclassified information in both the public and private sector, together with classified national security information systems of the military and intelligence establishment to create a seamless "national security interest" for which overall responsibility is placed in the hands of the National Security Agency.

While the ACLU understands the Administration's apparent desire to avoid piecemeal security policy-making, and would not quarrel with its choice of NSA as the lead agency for security policy in connection with classified national security information systems, we read NSDD 145 and its designation of the Director of NSA as the "National Manager for Telecommunications and Automated Information Systems Security" as mandating an unprecedented, unwise and uncheckable primacy of the Nation's national security apparatus in information policy -- an area where the balanced consideration of values other than "security" is of paramount importance to our system of government.

The ACLU's concerns are based upon our reading of NSA's authority under NSDD 145; the implications of such authority in light of NSA's primary mission; and, the absence of a broad contrapuntal role for non-national security elements of the Executive Branch. Our conclusions on these matters, or, more precisely, the issues that we raise, point to the need for coherent Congressional involvement and direction in the implementation of NSDD 145 so that improvements in T&AIS security are not purchased at the expense of an informed public and protections for individual personal privacy.

NSA Authority As "National Manager" Under NSDD 145

In sweeping terms, NSDD 145 designates the Director of NSA as "the government focal point" for T&AIS security policy, Sec.7.b., with authority to "review and approve all standards, techniques, systems and equipment" for T&AIS security, Sec.7.d.; "assess the overall security posture and disseminate information on hostile threats" to T&AIS security, Sec.7.g.; "prescribe the minimum standards, methods and procedures for protecting" T&AIS, Sec.7.i.; and, "review and assess annually" the T&AIS security programs and budgets of all agencies and departments of the government, Sec.7.j.

The scope of its authority to enter directly into the T&AIS operations of all federal agencies and departments is broad in its literal terms and subject to expansion through its ambiguity. In Sec.7.a., the National Manager is granted authority to "examine government [T&AIS] and evaluate their vulnerability to hostile interception and exploitation," if necessary by means which may include "monitoring of official telecommunications."

Neither the reasons for, nor the meaning of, this power to "examine" agency T&AIS first hand is explained.

The NSA is also authorized to "request from the heads of departments and agencies such information and technical support as may be needed to discharge the responsibilities assigned" to the National Manager. Sec.7.1. For their part, the heads of federal departments and agencies are ordered to "provide to... the National Manager... such information as may be required to discharge responsibilities assigned" to that office. Sec.8.c.

Finally, NSA's ability to influence the overall program is enhanced by the requirement that it provide "facilities and support" to, as well as staff to the "permanent secretariat" of, the National Telecommunications and Information Systems Security Committee (NTISSC) -- the umbrella group of specified agency representatives charged with development of "such specific operating policies, objectives, and priorities as may be required to implement" NSDD 145. Sec.5.d.

NSA influence in the NTISSC could have profound implications both inside and outside the federal government if concentrated with respect to the NTISSC's duty to "identify systems which handle sensitive, non-government information, the loss and exploitation of which could adversely affect the national security interest, for the purpose of encouraging, advising and, where appropriate, assisting the private sector in applying security measures." Sec.7.b.4.

Issues Raised By NSA's Authority and Other Aspects of NSDD 145

The pervasive theory of NSDD 145, which underscores ACLU concerns about the authority delegated to the NSA, is a view of "national security information" that reaches far beyond President Reagan's Executive Order 12356 on Classification to encompass a seemingly unbounded range of non-classified information in civilian T&AIS operations of both the public and private sector.

The effort to embrace security against T&AIS threats to "private or proprietary information of US persons and businesses" from "criminal elements", "terrorist groups", and "foreign exploitation" -- along with the obviously appropriate concern for compromise of classified information by "hostile intelligence services" -- has led the drafters of NSDD 145 to indulge the Administration's already disturbing penchant toward secrecy by presuming a need and authority for expansion of the universe of information properly subject to government security controls.

This awkward but determined straining of the "national security" rubric beyond its recognized limits is evident in repeated vague references to "sensitive" information and in the statement that "[s]uch information, even if unclassified in isolation, often can reveal highly classified and other sensitive information when taken in aggregate."

Moreover, its mischievous potential in blurring established laws and policies is manifest in the unclear policy distinction drawn between the indication that "classified national security information" shall be secured "by such means as are necessary to prevent compromise and exploitation," while "other sensitive, but unclassified, government or government-derived information, the loss of which could adversely affect the national security interest, shall be protected in proportion to the threat of exploitation and the associated potential damage to the national security." Sec.2.b.

The Administration's efforts to expand the category of "national security information" were not well received when they were entertained in the context of the drafting of President Reagan's Executive Order 12356 on Classification. New initiatives to achieve the same results through indirect policies should be even more forcefully rejected, especially at a time when it is clear that the Government is already attempting to protect far too much information "in the interest of national security." What do the terms used in NSDD 145 mean? What kind of "sensitive" information is at issue? If this information is in the private sector, is it privately-owned and generated? What is "government-derived information?"

These questions, based upon NSDD 145's broad yet ambiguous perspective on what kinds of information require the special T&AIS security expertise of the national security establishment, lead directly to a related inquiry about the impact on policies and operations in the civilian private and public sectors that may result from making the NSA the "government focal point" for implementation of NSDD 145.

It is not necessary to recite the litany of unlawful and improper NSA activities disclosed in Congressional hearings of the mid-1970s; the wholesale violation of the privacy rights of hundreds of thousands of Americans in the sweeping "Watch List" program known as Operation Minaret and the acquisition of millions of private cable communications under Operation Shamrock are a well-known part of an historical record of intelligence agency abuses that led to the creation of Congressional oversight committees, the enactment of specific statutory authorities such as the Foreign Intelligence Surveillance Act, and an ongoing effort to instill accountability into the intelligence process.

Although NSA still lacks a legislative charter and is still very much an executive creation whose activities are cloaked in extraordinary secrecy, it is not necessary to impute to NSA any residual lawlessness or "bad faith" motivation to question the wisdom of its designated role in NSDD 145's scheme for a "comprehensive and coordinated approach" toward T&AIS security throughout the federal government and the private sector as well. Assuming the best intentions on NSA's part, it still must be asked:

> * Do NSA's priorities within the military/intelligence establishment inherently conflict with its role as "focal point" for T&AIS security for all government agencies and the private sector under NSDD 145?
>
> * Will its policies in its role as National Manager be reflective of its primary military/intelligence mission, or will its advice be measured to lesser security needs?

* Will NSA's job-related disposition toward secrecy lead it to perform its duties under NSDD 145 with the same avoidance of public scrutiny that marks its day-to-day performance of its primary responsibilities?

* Is NSA's expertise perhaps too arcane for the actual needs of most non-national security agencies, in the sense that the best security programs might well be developed by those in each agency who are most familiar with that particular agency's systems and responsibilities?

It is clear that NSA itself cannot reasonably be expected to insure that considerations for open government and personal privacy are carefully balanced against perceived exploitation threats in devising sound T&AIS security policy; given the "national security" mindset that imbues NSDD 145, it is equally clear that the Directive offers no other source for such input within the the Executive Branch. This is perhaps just as well, since most advocates of these important values would be hard-pressed to recommend an Executive office, agency or department that has exhibited the ability or desire to effectively represent these interests in recent years.

Only the direct involvement of Congress can insure that openness and personal privacy considerations are given their full due in the development of T&AIS security policy. This is not, of course, an unusual role for Congress in light of its enactment of the Freedom of Information Act and the Privacy Act of 1974 -- measures aimed, respectively, at restricting Executive Branch discretion in denying public access to agency records and maintaining records in violation of an individual's right to personal privacy.

It may, however, require a new Congressional mechanism to deal coherently with the issues presented by NSDD 145. Recognition that T&AIS security policy reaches beyond the national security characterizations that artificially bind them in NSDD 145 to embrace a whole panoply of information and privacy issues brings with it the realization that these diverse but related issues are currently scattered among the jurisdictions of numerous committees and subcommittees in both houses of Congress. The Judiciary, Government Operations, and Intelligence committees of the House and Senate, together with other individual committees in both bodies, each have responsibilities for some aspect of the Government's information and privacy policies, but have shown no inclination or ability to coordinate their consideration of related issues.

It may now be time for Congress to create a Select Committee on Information which can, in the words of NSDD 145, take a "comprehensive and coordinated approach" to information and privacy policies. Congress cannot ignore NSDD 145, and it can find it a useful impetus for bringing order to its own "houses" for consideration of information and privacy issues in the face of current and future technological developments.

Mr. GLICKMAN. Thank you very much for your testimony.

The last witness today is Dr. John Richardson, member, Committee on Communications and Information Policy, Institute of Electrical and Electronics Engineers in Washington.

Sorry you have had to wait for so long. I must tell you, we may be having a vote in about 10 to 15 minutes. So, this is the way this place works, unfortunately, so if there is any way you can try to accelerate your statement, we would appreciate it, so you wouldn't have to wait until we came back.

STATEMENT OF JOHN M. RICHARDSON, MEMBER, COMMITTEE ON COMMUNICATIONS AND INFORMATION POLICY, INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS, INC., WASHINGTON, DC

Mr. RICHARDSON. I understand, Mr. Chairman.

Mr. Chairman, my name is John M. Richardson. I have a prepared statement which I would like to submit for the record, but I would like to cover the main points now orally.

I am a member of the Committee on Communications and Information Policy of the Institute of Electrical and Electronics Engineers. This committee is chaired by Dr. Lynn W. Ellis, who is also present in this room. My testimony is presented on behalf of that committee.

IEEE is the world's largest engineering society, with nearly 260,000 members worldwide, 214,000 of whom live and work in the United States. About 82 percent of our membership is employed in industry, 8 percent in academic institutions and 10 percent in the various Government laboratories and agencies. The IEEE Committee on Communications and Information Policy is vested with authority to develop the Institute's communications and information policy; and once those positions are adopted by the Institute, our Committee is one of the mechanisms by which the policy is voiced in public.

We thank you for the chance to present our views on the unclassified version of National Security Decision Directive 145, issued by the President on September 17, 1984.

NSDD 145 deals with three distinct aspects of the subject: One, classified information; two, other sensitive but unclassified Government or Government-derived information, the loss of which could adversely affect the national security interest; and three, sensitive non-Government information, the loss of which could also adversely affect national security .

We, too, recognize the need to protect the transmission and processing of information sensitive with respect to the commercial or the national security interests of the United States.5

But NSDD 145 raises certain questions for us. I will not comment on the protection of classified information, which is governed by existing law and Executive order. Similarly, I will have no comment on sensitive unclassified Government information which may be protected as the Government sees fit, as far as the IEEE is concerned. Rather, my statement will address five issues that NSDD 145 seems to raise with respect to unclassified, sensitive, non-Government information and private sector telecommunications and automated information systems.

First, how will one define the scope and the limits of the various categories of unclassified sensitive non-Government information without abridging the exchange of information throughout the private sector?

Second, how far does the proposed identification of private sector systems that handle sensitive Government and non-Government information extend?

Third, how may close coordination and information exchange between the private sector and the Government as to protection technology be established while avoiding restraints on technological initiatives and scientific communication that may be undertaken by private firms?

Fourth, does NSDD 145 contemplate the approval and the endorsement of private sector research and development, apart from contractual arrangements with the Government?

Fifth, does NSDD 145 contemplate that private sector systems will be subject to evaluation and certification, and if so, will this be on a voluntary or a mandatory basis?

The first issue I have mentioned is by far the most important, because it deals with the content of information itself. The remaining ones deal with the characteristics of the systems that contain or transmit the information and the extent of Government involvement with them.

The IEEE is concerned first, as to the feasibility in practice of attaining the objectives of NSDD 145, insofar as unclassified, non-Government information is concerned. The difficulty centers around the identification of sensitive information and the subsequent measures necessary to deal with it. Indeed, in the event that the protective efforts of the Systems Security Steering Group should ultimately extend to enforcement measures that may involve regulation, restraint, or monitoring, we see a real possibility of a collision with constitutional principles of individual privacy and freedom of speech.

Second, the IEEE is concerned at the extent to which the implementation of the directive seems to reach into the operation of private sector activities and systems. As this reach increases, so will the difficulties of identifying and evaluating the systems, and reviewing and endorsing the research of the private sector. The directive does not set the scope and the limits of its interaction with the private sector.

Third, as to scientific and technical information, with which the IEEE is especially concerned, the open dissemination of unclassified information is deemed crucial to the continued advancement of U.S. industry.

And finally, given that the policies of NSDD 145 greatly impact the private sector, we are concerned that private sector interests are not represented in the proposed implementation procedures.

For these reasons, IEEE recommends that the groups responsible for implementing NSDD 145 review the feasibility of, and exercise extreme restraint in, designating categories of sensitive, non-Government information. Certainly, there should be no effort to regulate or to control any such category. These groups should also exercise extreme restraint in efforts to identify and bring about the protection of private sector systems that handle non-Government information. Activities should be limited to alerting the private sector to the problem and encouraging appropriate private action. We also strongly urge, in view of the nature of the problem, that there be substantial representation by knowledgeable experts from the private sector on the Government committees implementing the directive.

Now, the remainder of the prepared statement addresses these five issues more fully. In that statement we have first quoted a particular provision of the directive that affects our organization. We have articulated the issue that it raises, and the statement comments briefly on it.

Mr. GLICKMAN. First of all, I want to thank you for the statement, because I have read through the last three pages, and I think that you make some excellent—you describe the issues and then comment on those issues as good as anything that I have seen to date.

As a matter of fact, I mention again, that all of the testimony today, from the first witness, the Secretary, to the National Security Agency to this, have been excellent in terms of focusing the problems directly, and I am appreciative for that.

I am concerned that the private sector has not been terribly—well, has not been intimately involved in this national security directive, which I think is implied in your statement. And that is one of the problems of doing it this way.

And I wonder how you feel procedurally. The private sector might have more input into the process. When I say the process, I mean technically, logistically and institutionally, in the Government.

Mr. RICHARDSON. One difficulty is that this directive is a sort of a hybrid in that it addresses a problem within the Government and a problem outside the Government.

It is difficult to have private citizens sitting as members of Government committees. If that proves a difficulty in this case, I think recourse will have to be had to the advisory committee mechanism. At the very least, this apparatus should establish an advisory committee on telecommunications and automated information systems security and give it full prominence, perhaps in the same way that the National Security Telecommunications Advisory Committee, NSTAC, has been constituted and woven into the Government mechanism.

Mr. GLICKMAN. Who does that committee advise?

Mr. RICHARDSON. NSTAC was a committee that was established by the President. I think it reports to the National Security Council through the President's National Security Advisor. It is rather intimately bound up with both the Office of Science and Technology Policy and the Defense Communications Agency.

Mr. GLICKMAN. But at the present time, you are not aware of any advisory committee structure to the committee that has been created by NSDD 145?

Mr. RICHARDSON. No, sir; I am not aware of any private advisory structure.

Mr. **Glickman**. Well, we appreciate very much your testimony, and do any of my colleagues have any questions? No questions?

Thank you very much for coming.

This hearing is adjourned. There will be a press conference in this room at 2:00 on an unrelated—well, related piece of legislation, not dealing with the directive, dealing with the National Bureau of Standards.

The hearing is adjourned.

[Whereupon, at 1:00 p.m., the subcommittee was adjourned.]

[The prepared statement of Mr. Richardson follows:]

1884 · 1984
A CENTURY OF ELECTRICAL PROGRESS

IEEE **TECHNICAL ACTIVITIES BOARD/UNITED STATES ACTIVITIES BOARD**
COMMITTEE ON COMMUNICATIONS AND INFORMATION POLICY

Lynn W. Ellis
Chairman
(203) 227-0345

Richard Gould
Vice Chairman
(202) 223-4449

Edith T. Carper
Executive Secretary
(202) 785-0017

PLEASE REPLY TO
12 Beechwood Lane
Westport, CT 06880 USA

STATEMENT OF
DR. JOHN M. RICHARDSON
on behalf of
THE COMMITTEE ON COMMUNICATIONS AND INFORMATION POLICY
of the
INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS
on
NATIONAL SECURITY DECISION DIRECTIVE 145

Before the Subcommittee on Transportation, Aviation and Materials
Committee on Science and Technology
United States House of Representatives

June 27, 1985

THE INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS, INC.
Headquarters: 345 East 47th Street, New York, N.Y. 10017 Area Code (212) 705-7900
Washington Office: 1111 19th St. NW, Washington, DC 20036 Area Code (202) 785-0017

STATEMENT OF
DR. JOHN M. RICHARDSON
on behalf of
THE COMMITTEE ON COMMUNICATIONS AND INFORMATION POLICY
of the
INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS
on
NATIONAL SECURITY DECISION DIRECTIVE 145

Before the Subcommittee on Transportation, Aviation and Materials
Committee on Science and Technology
United States House of Representatives

June 27, 1985

Mr. Chairman, my name is John M. Richardson, member of the Committee on Communications and Information Policy of the Institute of Electrical and Electronics Engineers (IEEE). My testimony is presented on behalf of that committee. The IEEE is the world's largest engineering society, with nearly 260,000 members worldwide, 214,000 of whom live and work in the United States. Approximately 82 percent of our membership is employed in industry, 8 percent in academic institutions, and 10 percent in the various government laboratories and agencies. The IEEE Committee on Communications and Information Policy is vested with authority to develop the Institute's communications and information policy; and, once that policy is adopted by the Institute, our committee is one of the major mechanisms by which the policy is voiced in public.

We thank you for the chance to present our views on the unclassified version of National Security Decision Directive (NSDD) 145, entitled "National Policy on Telecommunications and Automated Information Systems Security" and issued by the President on September 17, 1984. NSDD 145 deals with three distinct aspects of the subject: (1) classified information; (2) other sensitive, but unclassified, government or government-derived information, the loss of which could adversely affect the national security interest; and (3) sensitive non-government information, the loss of which could also adversely affect national security.

We, too, recognize an increasing need to protect the transmission and processing of information sensitive with respect to the commercial or the national security interests of the United States. Yet, NSDD 145 raises certain questions for us. I have no comment on the protection of classified information, which is governed by existing law and Executive Order. Similarly, I have no comment on sensitive, unclassified government information, which may be protected as the government sees fit. Rather, my statement will address five issues that NSDD 145 seems to raise with respect to unclassified, sensitive, non-government information and private-sector telecommunications and automated information systems.

1. How will one define the scope and limits of various categories of unclassified, sensitive, non-government information without abridging the exchange of information throughout the private sector?

2. How far does the proposed identification of private sector systems that handle sensitive government and non-government information extend?

3. How may close coordination and information exchange between the private sector and the government in protection technology be established while avoiding restraints on technological initiatives and scientific communication that may be undertaken by private firms?

4. Does NSDD 145 contemplate approval and endorsement of private sector research and development apart from contractual arrangements?

5. Does NSDD 145 contemplate that private sector systems will be subject to evaluation and certification, and, if so, on a voluntary or mandatory basis?

The first issue deals with the content of information itself. The remaining ones deal with the characteristics of systems that contain or transmit information and the extent of government involvement with them.

IEEE is concerned first as to the feasibility, in actual practice, of attaining the objectives of NSDD 145 insofar as unclassified, non-government information is concerned. The difficulty centers around the identification of "sensitive information" and the subsequent measures necessary to deal with it. Indeed, in the event that the protective efforts of the Systems Security Steering Group should ultimately extend to enforcement measures that may involve regulation, restraint, and monitoring, we see a real possibility of collision with constitutional principles of individual privacy and freedom of speech.

Secondly, IEEE is concerned at the extent to which the implementation of NSDD 145 seems to reach into the operation of private sector activities and systems. As the reach increases, so will the difficulties of identifying and evaluating systems and of reviewing and endorsing research in the private sector. NSDD 145 does not set the scope and limits of its interaction with the private sector.

Thirdly, as to scientific and technical information, with which the IEEE is particularly concerned, the open dissemination of unclassified information is deemed crucial to the continued advancement of U.S. industry.

Finally, given that the policies of NSDD 145 greatly impact the private sector, we are concerned that private interests are not represented in the proposed implementation procedures.

For these reasons IEEE recommends that the groups responsible for implementing NSDD 145 review the feasibility of, and exercise extreme restraint in, designating categories of sensitive, non-government information. Certainly there should be no effort to regulate or control any such category. These groups should also exercise extreme restraint in efforts to identify and bring about the protection of private-sector systems that handle non-government information. Activities should be limited to alerting the private sector to the problem and encouraging appropriate private action. We also strongly urge, in view of the nature of the problem, that there be substantial representation by knowledgeable experts from the private sector on the government committees implementing the Directive.

The remainder of this statement addresses the five issues more fully. In each of the following numbered paragraphs, we have first noted a particular provision of NSDD 145 that affects our organization, then identified an issue raised by the provision, and finally commented briefly on it.

1. Characterization of Unclassified, Sensitive, Non-government Information

   Provision: NSDD 145 provides that the Systems Security Steering Group shall "[i]dentify categories of sensitive non-government information, the loss of which could adversely affect the national security interest, and recommend steps to protect such information." [Section 4.a.(10)]

   Issue: The issue is how to define the scope and limits of these categories without abridgement of the exchange of information throughout the private sector.

   Comment: Although the objective of identifying such categories of sensitive non-government information with a view to protecting them may appear attractive to some, we believe that almost insuperable difficulties surround the task because of the great variety and pervasiveness of information flow within our society. The boundaries of any such categories are inevitably diffuse and cannot be characterized with precision. Thus there is a risk of casting too wide a net in carrying out this provision of NSDD 145. The provision may turn out to be, at worst, excessively intrusive and inhibitive and, at best, ineffectual. Indeed, experience with analogous efforts under a prior Presidential Directive did prove ineffectual.

2. Identification of Private-Sector Systems That Handle Sensitive Government and Non-government Information

   Provision: NSDD 145 provides that the National Telecommunications and Information Systems Security Committee shall "[s]ubmit annually to the Steering Group an evaluation of the status of national telecommunications and automated information systems security with respect to established objectives and priorities" [Section 5.b.(3)] and "[i]dentify systems which handle sensitive, non-government information, the loss and exploitation of which could adversely affect the national security interest, for the purpose of encouraging, advising and, where appropriate, assisting the private sector in applying security measures." [Section 5.b.(4)]

   Issue: The issue is how far this mandate extends into private sector systems. Presumably, the "established objectives" cited above embrace "sensitive, but unclassified, government or government-derived information, the loss of which could adversely affect the national security interest." [Section 2.b.]

   Comment: The mix and proliferation of private, commercial, government, and government-derived information is widespread throughout both the leased and the public switched networks. Therefore, it would be an extremely complex undertaking to identify individual commercial and private sector telecommunications circuits that handle sensitive non-government information. The government would have to rely on the full involvement of the private sector in this effort. The government would also have to provide assurances that its methods of identification are nonintrusive and in compliance with law.

3. Support for a Technical Base Within the Private Sector

Provision: NSDD 145 states that one of its objectives is to provide for "...support for a superior technical base within the private sector in areas which complement and enhance government capabilities" [Section 1.b.] and "...encouragement of private sector security initiatives." [Section 1.c.]

Issue: The issue is how to establish close coordination and information exchange between the private sector and the government in this technology while avoiding restraints on the technological initiatives and their applications that may be undertaken by the private sector.

Comment: We endorse the provision of technical support in this area as essential to national goals. However, experience with support for research and technology in other areas related to national security has shown that it is hard to manage the exchange of unclassified information in ways that satisfy both the government and the technical community. We advise against further restraints on unclassified information.

4. Approval and Endorsement of Research

Provision: NSDD 145 provides that the Executive Agent of the Government for Telecommunications and Information Systems Security and the National Manager for Telecommunications Security and Automated Information Systems Security shall "[c]onduct, approve, or endorse research and development of techniques and equipment for telecommunications and automated information systems security for national security information." [Section 6.d. and Section 7.c.]

Issue: The issue is the extent to which the Executive Agent and the National Manager may approve research and development in the private sector. The context of the provisions seems to indicate that these functions are to be exercised only within the government for national security information. However, the concern of NSDD 145 with private sector activities may allow an interpretation that private sector research is subject to approval.

Comment: Approval and endorsement of research in the private sector should occur only in connection with the normal contractual arrangements between the government and the performers of research. We urge the Executive Agent and the National Manager to make this point clear.

5. Evaluation and Certification of System Security

Provision: NSDD 145 provides that the National Manager for Telecommunciations Security and Automated Information Systems Security shall have authority to "[o]perate a central technical center to evaluate and certify the security of telecommunications systems and automated information systems." [Section 7.h.]

Issue: The issue is whether evaluation and certification of private sector systems are contemplated, and, if so, whether on a voluntary or mandatory basis for the system operator. The context of the provision seems to indicate that these functions are to be exercised only within the government. However, the concern of NSDD 145 with private sector activities may allow an interpretation that private sector systems are subject to evaluation and certification.

Comment: Mandatory evaluation and certification of private sector systems that do not handle classified information are inappropriate and raise problems of scope and limitations in view of the proliferation of systems and information noted under point (2) above. We urge the National Manager to clarify this point.

Mr. Chairman, thank you for your attention to our statement. I will be happy to address any question that you or the Members may have.